



Documentazione Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

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

Sommario

Documentazione Active IQ Unified Manager	1
Note di rilascio	2
Iniziare	3
Istruzioni di avvio rapido per le installazioni VMware	3
Requisiti di sistema	3
Installa Active IQ Unified Manager	3
Istruzioni rapide per l'installazione di Linux	4
Requisiti di sistema	4
Installa Active IQ Unified Manager	4
Istruzioni di avvio rapido per le installazioni di Windows	5
Requisiti di sistema	5
Installa Active IQ Unified Manager	6
Installa Unified Manager sui sistemi VMware vSphere	7
Introduzione ad Active IQ Unified Manager	7
Cosa fa il server Unified Manager	7
Panoramica della sequenza di installazione	7
Requisiti per l'installazione di Unified Manager	8
Requisiti di sistema hardware e infrastruttura virtuale	8
Requisiti software e di installazione VMware	9
Browser supportati	10
Requisiti di protocollo e porta	11
Completa il foglio di lavoro	14
Installa, aggiorna e rimuovi il software Unified Manager	16
Panoramica del processo di distribuzione	16
Distribuisci Unified Manager	17
Aggiorna Unified Manager	21
Riavviare la macchina virtuale Unified Manager	24
Rimuovi Unified Manager	24
Installa Unified Manager sui sistemi Linux	25
Introduzione ad Active IQ Unified Manager	25
Cosa fa il server Unified Manager	25
Panoramica della sequenza di installazione	25
Requisiti per l'installazione di Unified Manager	26
Requisiti di sistema hardware e infrastruttura virtuale	26
Requisiti di installazione e software Linux	28
Browser supportati	30
Requisiti di protocollo e porta	31
Completa il foglio di lavoro	34
Installa, aggiorna e rimuovi il software Unified Manager	36
Panoramica del processo di installazione	36
Impostare i repository software richiesti	37
Requisiti SELinux sulle condivisioni NFS e CIFS	38
Installa Unified Manager sui sistemi Linux	41

Aggiorna Unified Manager su Red Hat Enterprise Linux	48
Aggiornare i prodotti di terze parti dopo l'installazione di Unified Manager	53
Riavvia Unified Manager	53
Rimuovi Unified Manager	54
Rimuovere l'utente umadmin personalizzato e il gruppo di manutenzione	55
Installa Unified Manager sui sistemi Windows	56
Introduzione ad Active IQ Unified Manager	56
Cosa fa il server Unified Manager	56
Panoramica della sequenza di installazione	56
Requisiti per l'installazione di Unified Manager	57
Requisiti di sistema hardware e infrastruttura virtuale	57
Requisiti di installazione e software Windows	59
Browser supportati	60
Requisiti di protocollo e porta	61
Completa il foglio di lavoro	64
Installa, aggiorna e rimuovi il software Unified Manager	66
Panoramica del processo di installazione	66
Installa Unified Manager su Windows	66
Cambia la password di JBoss	70
Percorso di aggiornamento supportato per le versioni di Unified Manager	70
Aggiorna Unified Manager	71
Aggiornare i prodotti di terze parti	73
Disinstallare i prodotti di terze parti	74
Riavvia Unified Manager	74
Disinstallare Unified Manager	75
Eseguire attività di configurazione e amministrative	77
Configura Active IQ Unified Manager	77
Panoramica della sequenza di configurazione	77
Accedi all'interfaccia utente web di Unified Manager	77
Eseguire la configurazione iniziale dell'interfaccia utente Web di Unified Manager	78
Aggiungi cluster	80
Configurare Unified Manager per inviare notifiche di avviso	82
Cambia la password dell'utente locale	91
Imposta il timeout di inattività della sessione	91
Imposta il timeout della sessione tramite CLI	92
Cambiare il nome host di Unified Manager	92
Abilitare e disabilitare la gestione dell'archiviazione basata su policy	97
Configurare il backup di Unified Manager	98
Gestisci le impostazioni delle funzionalità	98
Abilita la gestione dell'archiviazione basata su policy	99
Abilita API Gateway	99
Specificare il timeout di inattività	100
Abilita gli eventi del portale Active IQ	100
Abilita e disabilita le impostazioni di sicurezza per la conformità	101
Abilita e disabilita il caricamento degli script	102

Aggiungi banner di accesso	102
Utilizzare la console di manutenzione	102
Quali funzionalità fornisce la console di manutenzione	102
Cosa fa l'utente addetto alla manutenzione	103
Capacità diagnostiche dell'utente	103
Accedi alla console di manutenzione	103
Accedi alla console di manutenzione tramite la console vSphere VM	104
Menu della console di manutenzione	105
Cambiare la password dell'utente di manutenzione su Windows	110
Cambiare la password umadmin sui sistemi Linux	110
Modifica le porte utilizzate da Unified Manager per i protocolli HTTP e HTTPS	111
Aggiungere interfacce di rete	111
Aggiungere spazio su disco alla directory del database Unified Manager	112
Gestisci l'accesso degli utenti	116
Aggiungi utenti	116
Modifica le impostazioni utente	117
Visualizza utenti	118
Elimina utenti o gruppi	118
Che cosa è RBAC	118
Cosa fa il controllo degli accessi basato sui ruoli	118
Definizioni dei tipi di utente	119
Definizioni dei ruoli utente	119
Ruoli e capacità degli utenti di Unified Manager	120
Gestisci le impostazioni di autenticazione SAML	122
Requisiti del fornitore di identità	123
Abilita l'autenticazione SAML	124
Cambia il provider di identità utilizzato per l'autenticazione SAML	125
Aggiorna le impostazioni di autenticazione SAML dopo la modifica del certificato di sicurezza di Unified Manager	126
Disabilitare l'autenticazione SAML	127
Disabilitare l'autenticazione SAML dalla console di manutenzione	128
Pagina di autenticazione SAML	128
Gestisci l'autenticazione	129
Modifica i server di autenticazione	129
Elimina i server di autenticazione	130
Autenticazione con Active Directory o OpenLDAP	130
Registrazione di controllo	131
Pagina di autenticazione remota	133
Gestire i certificati di sicurezza	137
Visualizza il certificato di sicurezza HTTPS	137
Scarica una richiesta di firma del certificato HTTPS	137
Installa un certificato HTTPS firmato e restituito da una CA	137
Installa un certificato HTTPS generato utilizzando strumenti esterni	138
Descrizioni delle pagine per la gestione dei certificati	141
Monitorare e gestire l'archiviazione	144

Introduzione ad Active IQ Unified Manager	144
Introduzione al monitoraggio dello stato di salute Active IQ Unified Manager	144
Introduzione al monitoraggio delle prestazioni Active IQ Unified Manager	145
Utilizzare le API REST di Unified Manager	146
Cosa fa il server Unified Manager	146
Comprendere l'interfaccia utente	147
Tipiche disposizioni delle finestre	147
Personalizzazione del layout della finestra	148
Utilizzare la Guida di Unified Manager	149
Aggiungi ai preferiti i tuoi argomenti della Guida preferiti	150
Cerca oggetti di archiviazione	150
Esportare i dati di archiviazione come report	151
Filtra il contenuto della pagina dell'inventario	153
Visualizza gli eventi attivi dalla campana delle notifiche	154
Monitora e gestisci i cluster dalla dashboard	154
Pagina del dashboard	155
Gestisci i problemi o le funzionalità ONTAP direttamente da Unified Manager	158
Gestire i cluster	166
Come funziona il processo di scoperta del cluster	166
Visualizza l'elenco dei cluster monitorati	167
Aggiungi cluster	167
Modifica cluster	170
Rimuovi i cluster	170
Riscoprire i cluster	171
Monitorare l'infrastruttura virtuale VMware	171
Cosa non è supportato	174
Visualizza e aggiungi vCenter Server	175
Rimuovere vCenter Server	177
Monitorare le macchine virtuali	177
Visualizza l'infrastruttura virtuale in una configurazione di disaster recovery	179
Fornire e gestire i carichi di lavoro	181
Panoramica dei carichi di lavoro	182
Livelli di servizio prestazionali	189
Gestire le policy di efficienza dello storage	195
Gestire e monitorare le configurazioni MetroCluster	197
Comportamento del volume durante la commutazione e la commutazione indietro	197
Definizioni dello stato di connettività del cluster per MetroCluster sulla configurazione FC	199
Definizioni dello stato di mirroring dei dati per MetroCluster su FC	200
Monitorare le configurazioni MetroCluster	201
Monitorare la replica MetroCluster	204
Gestire le quote	205
Quali sono i limiti delle quote	205
Visualizza le quote degli utenti e dei gruppi di utenti	205
Crea regole per generare indirizzi email	205
Creare un formato di notifica e-mail per le quote degli utenti e dei gruppi di utenti	206

Modifica gli indirizzi email delle quote utente e gruppo	207
Scopri di più sulle quote	207
Descrizione delle finestre di dialogo delle quote	208
Risoluzione dei problemi	211
Aggiungere spazio su disco alla directory del database Unified Manager	212
Modificare l'intervallo di raccolta delle statistiche sulle prestazioni	215
Modificare la durata del periodo di conservazione dei dati sugli eventi e sulle prestazioni da parte di Unified Manager	216
Errore di autenticazione sconosciuto	217
Utente non trovato	217
Problema con l'aggiunta di LDAP tramite altri servizi di autenticazione	217
Problema di rotazione dei log di NetApp Manageability SDK sui sistemi Windows	218
Gestisci eventi e avvisi	219
Gestire gli eventi	219
Cosa sono gli eventi della piattaforma Active IQ	219
Cosa sono gli eventi del sistema di gestione degli eventi	219
Cosa succede quando viene ricevuto un evento	225
Visualizza gli eventi e i dettagli dell'evento	226
Visualizza eventi non assegnati	227
Riconoscere e risolvere gli eventi	227
Assegna eventi a utenti specifici	228
Disabilitare gli eventi indesiderati	229
Risolvi i problemi utilizzando la correzione automatica di Unified Manager	230
Abilita e disabilita la segnalazione degli eventi Active IQ	231
Carica un nuovo file di regole Active IQ	232
Come vengono generati gli eventi della piattaforma Active IQ	233
Risolvi gli eventi della piattaforma Active IQ	233
Configurare le impostazioni di conservazione degli eventi	234
Cos'è una finestra di manutenzione di Unified Manager	234
Gestire gli eventi delle risorse del sistema host	237
Scopri di più sugli eventi	237
Elenco degli eventi e dei tipi di gravità	243
Descrizione delle finestre degli eventi e delle finestre di dialogo	303
Gestisci gli avvisi	315
Cosa sono gli avvisi	315
Quali informazioni sono contenute in un'e-mail di avviso	316
Aggiungi avvisi	316
Aggiungi avvisi per eventi di performance	319
Avvisi di prova	320
Abilita e disabilita gli avvisi per gli eventi Risolti e Obsoleti	321
Escludere i volumi di destinazione del ripristino di emergenza dalla generazione di avvisi	321
Visualizza avvisi	322
Modifica avvisi	322
Elimina avvisi	323
Descrizione delle finestre di avviso e delle finestre di dialogo	323

Gestisci gli script	329
Come funzionano gli script con gli avvisi	329
Aggiungi script	330
Elimina gli script	331
Esecuzione dello script di test	332
Comandi CLI di Unified Manager supportati	332
Descrizione delle finestre di script e delle finestre di dialogo	338
Monitorare e gestire le prestazioni del cluster	340
Introduzione al monitoraggio delle prestazioni Active IQ Unified Manager	340
Funzionalità di monitoraggio delle prestazioni di Unified Manager	340
Interfacce Unified Manager utilizzate per gestire le prestazioni del sistema di archiviazione	341
Attività di raccolta dati sulla configurazione e sulle prestazioni del cluster	341
Cos'è un ciclo di raccolta della continuità dei dati	343
Cosa significa il timestamp nei dati e negli eventi raccolti	344
Esplora i flussi di lavoro delle prestazioni nell'interfaccia utente grafica di Unified Manager	344
Accedi all'interfaccia utente	344
Interfaccia grafica e percorsi di navigazione	345
Cerca oggetti di archiviazione	350
Filtra il contenuto della pagina dell'inventario	351
Monitorare le prestazioni del cluster dalla Dashboard	353
Comprendere i pannelli delle prestazioni nella Dashboard	353
Messaggi e descrizioni dei banner sulle prestazioni	354
Modificare l'intervallo di raccolta delle statistiche sulle prestazioni	354
Risolvi i problemi dei carichi di lavoro utilizzando l'analizzatore dei carichi di lavoro	355
Quali dati visualizza l'analizzatore del carico di lavoro?	356
Quando dovrei usare l'analizzatore del carico di lavoro?	357
Utilizzare l'analizzatore del carico di lavoro	358
Monitora le prestazioni del cluster dalla pagina di destinazione del cluster delle prestazioni	358
Comprendere la pagina di destinazione del Performance Cluster	358
Pagina di destinazione del Performance Cluster	359
Monitorare le prestazioni utilizzando le pagine Inventario delle prestazioni	364
Visualizza le pagine dell'inventario delle prestazioni per tutti gli oggetti di archiviazione	365
Contenuto della pagina dell'inventario delle prestazioni di raffinazione	370
Comprendere le raccomandazioni di Unified Manager per suddividere i dati nel cloud	373
Monitorare le prestazioni utilizzando le pagine di Performance Explorer	374
Comprendere l'oggetto radice	374
Applica il filtro per ridurre l'elenco degli oggetti correlati nella griglia	375
Specificare un intervallo di tempo per gli oggetti correlati	375
Definire l'elenco degli oggetti correlati per la creazione di grafici di confronto	377
Comprendere i grafici dei contatori	378
Tipi di grafici contatori delle prestazioni	379
Seleziona i grafici delle prestazioni da visualizzare	381
Espandi il riquadro Grafici contatore	382
Cambia il focus dei grafici dei contatori in un periodo di tempo più breve	382
Visualizza i dettagli dell'evento nella cronologia degli eventi	383

Visualizzazione zoom dei grafici dei contatori	384
Visualizza la latenza del volume per componente del cluster	386
Visualizza il traffico IOPS SVM per protocollo	387
Visualizza i grafici di volume e latenza LUN per verificare la garanzia delle prestazioni	388
Visualizza le prestazioni per tutti i cluster SAN Array	388
Visualizza gli IOPS del nodo in base ai carichi di lavoro che risiedono solo sul nodo locale	389
Componenti delle landing page degli oggetti	389
Gestire le prestazioni utilizzando le informazioni del gruppo di policy QoS	395
Come la qualità del servizio di archiviazione può controllare la produttività del carico di lavoro	395
Visualizza tutti i gruppi di policy QoS disponibili su tutti i cluster	397
Visualizza volumi o LUN che si trovano nello stesso gruppo di policy QoS	397
Visualizza le impostazioni del gruppo di criteri QoS applicate a volumi o LUN specifici	398
Visualizza i grafici delle prestazioni per confrontare volumi o LUN che si trovano nello stesso gruppo di policy QoS	399
Come vengono visualizzati i diversi tipi di policy QoS nei grafici di throughput	399
Visualizza le impostazioni minime e massime della qualità del servizio del carico di lavoro in Performance Explorer	401
Gestire le prestazioni utilizzando la capacità delle prestazioni e le informazioni IOPS disponibili	402
Quale capacità di prestazione è utilizzata	402
Cosa significa il valore della capacità prestazionale utilizzata	403
Quali IOPS sono disponibili	404
Visualizza i valori utilizzati per la capacità di prestazione aggregata e del nodo	405
Visualizza i nodi e aggrega i valori IOPS disponibili	406
Visualizza i grafici del contatore della capacità di prestazione per identificare i problemi	407
Capacità prestazionale utilizzata, condizioni di soglia prestazionale	409
Utilizzare il contatore della capacità di prestazione utilizzata per gestire le prestazioni	410
Comprendere e utilizzare la pagina Pianificazione del failover dei nodi	411
Utilizzare la pagina Pianificazione del failover del nodo per determinare le azioni correttive	411
Componenti della pagina Pianificazione del failover del nodo	411
Utilizzare una politica di soglia con la pagina Pianificazione del failover del nodo	413
Utilizzare il grafico di ripartizione della capacità di prestazione utilizzata per la pianificazione del failover	413
Raccogli dati e monitora le prestazioni del carico di lavoro	415
Tipi di carichi di lavoro monitorati da Unified Manager	415
Valori di misurazione delle prestazioni del carico di lavoro	416
Qual è l'intervallo di prestazioni previsto	418
Come viene utilizzata la previsione della latenza nell'analisi delle prestazioni	419
Come Unified Manager utilizza la latenza del carico di lavoro per identificare i problemi di prestazioni	420
Come le operazioni del cluster possono influenzare la latenza del carico di lavoro	421
Monitoraggio delle prestazioni delle configurazioni MetroCluster	422
Comprendere gli eventi e gli avvisi sulle prestazioni	423
Fonti degli eventi di performance	423
Tipi di gravità degli eventi prestazionali	424
Modifiche alla configurazione rilevate da Unified Manager	425
Tipi di criteri di soglia delle prestazioni definiti dal sistema	425

Analisi e notifica degli eventi prestazionali	428
Come Unified Manager determina l'impatto sulle prestazioni di un evento	430
Componenti del cluster e perché possono essere in competizione	430
Ruoli dei carichi di lavoro coinvolti in un evento di performance	432
Gestire le soglie di prestazione	434
Come funzionano i criteri di soglia delle prestazioni definiti dall'utente	434
Cosa succede quando viene violata una soglia di prestazione	436
Quali contatori delle prestazioni possono essere monitorati utilizzando le soglie	436
Quali oggetti e contatori possono essere utilizzati nelle policy di soglia combinate	439
Creare criteri di soglia delle prestazioni definiti dall'utente	439
Assegnare criteri di soglia delle prestazioni agli oggetti di archiviazione	441
Visualizza i criteri di soglia delle prestazioni	442
Modificare i criteri di soglia delle prestazioni definiti dall'utente	442
Rimuovere i criteri di soglia delle prestazioni dagli oggetti di archiviazione	443
Cosa succede quando viene modificata una politica di soglia di prestazione	443
Cosa succede alle policy di soglia delle prestazioni quando un oggetto viene spostato	444
Analizza gli eventi di performance	445
Visualizza informazioni sugli eventi di performance	445
Analizza gli eventi dalle soglie di prestazioni definite dall'utente	446
Analizza gli eventi dalle soglie di prestazione definite dal sistema	447
Analizza gli eventi dalle soglie di prestazioni dinamiche	453
Risolvere gli eventi di performance	461
Verificare che la latenza sia compresa nell'intervallo previsto	461
Esaminare l'impatto delle modifiche alla configurazione sulle prestazioni del carico di lavoro	461
Opzioni per migliorare le prestazioni del carico di lavoro dal lato client	461
Verificare la presenza di problemi con il client o con la rete	462
Verificare se altri volumi nel gruppo di policy QoS presentano un'attività insolitamente elevata	462
Spostare le interfacce logiche (LIF)	463
Eseguire operazioni di efficienza di archiviazione in orari meno impegnativi	463
Aggiungi dischi e rialloca i dati	464
Come l'abilitazione della Flash Cache su un nodo può migliorare le prestazioni del carico di lavoro	465
Come l'abilitazione di Flash Pool su un aggregato di storage può migliorare le prestazioni del carico di lavoro	465
Controllo dello stato di integrità della configurazione MetroCluster	465
Verifica della configurazione MetroCluster	466
Spostare i carichi di lavoro su un aggregato diverso	466
Spostare i carichi di lavoro su un nodo diverso	468
Spostare i carichi di lavoro su un aggregato su un nodo diverso	469
Spostare i carichi di lavoro su un nodo in una coppia HA diversa	471
Spostare i carichi di lavoro su un altro nodo in una coppia HA diversa	472
Utilizzare le impostazioni dei criteri QoS per dare priorità al lavoro su questo nodo	474
Rimuovere volumi e LUN inattivi	475
Aggiungere dischi ed eseguire la ricostruzione del layout aggregato	475
Impostare una connessione tra un server Unified Manager e un provider di dati esterno	475
Dati sulle prestazioni che possono essere inviati a un server esterno	476

Configura Graphite per ricevere dati sulle prestazioni da Unified Manager	477
Configurare una connessione da un server Unified Manager a un provider di dati esterno	478
Monitorare e gestire lo stato di salute del cluster	480
Introduzione al monitoraggio dello stato di salute Active IQ Unified Manager	480
Capacità fisica e logica	480
Unità di misura della capacità	480
Funzionalità di monitoraggio dello stato di Unified Manager	481
Interfacce di Unified Manager utilizzate per gestire lo stato del sistema di archiviazione	482
Gestione e monitoraggio dei cluster e dello stato degli oggetti cluster	483
Comprendere il monitoraggio dei cluster	483
Visualizza l'elenco e i dettagli dei cluster	485
Controllare lo stato dei cluster in una configurazione MetroCluster	485
Visualizza lo stato di integrità e capacità di tutti i cluster SAN Array	487
Visualizza l'elenco dei nodi e i dettagli	488
Generare un report di inventario hardware per il rinnovo del contratto	489
Visualizza l'elenco e i dettagli delle VM di archiviazione	489
Visualizza l'elenco aggregato e i dettagli	490
Visualizza le informazioni sulla capacità FabricPool	490
Visualizza i dettagli del pool di archiviazione	492
Visualizza l'elenco dei volumi e i dettagli	492
Visualizza i dettagli sulle azioni NFS	493
Visualizza i dettagli sulle azioni SMB/CIFS	494
Visualizza l'elenco delle copie Snapshot	495
Elimina le copie Snapshot	495
Calcola lo spazio recuperabile per le copie Snapshot	496
Descrizione delle finestre e delle finestre di dialogo degli oggetti cluster	497
Flussi di lavoro e attività sanitarie comuni di Unified Manager	497
Monitorare e risolvere i problemi di disponibilità dei dati	498
Risolvere i problemi di capacità	505
Gestire le soglie di salute	507
Gestire gli obiettivi di sicurezza del cluster	512
Gestire le operazioni di backup e ripristino	524
Gestisci gli script	540
Gestire e monitorare i gruppi	543
Assegnare la priorità agli eventi degli oggetti di archiviazione utilizzando le annotazioni	551
Invia 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
Creare, monitorare e risolvere i problemi delle relazioni di protezione	625
Tipi di protezione SnapMirror	625
Impostare le relazioni di protezione in Unified Manager	627
Eseguire un failover e un failback della relazione di protezione	629
Risolvere un errore del processo di protezione	633
Risolvere i problemi di ritardo	636
Gestire e monitorare le relazioni di protezione	638

Visualizza lo stato di protezione del volume	638
Visualizza le relazioni di protezione del volume	640
Monitorare i LUN in una relazione di gruppo di coerenza	641
Creare una relazione di protezione SnapVault dalla vista Integrità: Tutti i volumi	642
Crea una relazione di protezione SnapVault dalla pagina dei dettagli Volume/Stato	643
Creare una relazione di protezione SnapMirror dalla vista Integrità: Tutti i volumi	644
Crea una relazione di protezione SnapMirror dalla pagina dei dettagli Volume/Stato	645
Crea una relazione SnapMirror con replica flessibile in base alla versione	646
Crea relazioni SnapMirror con replica flessibile in base alla versione con opzione di backup	647
Configurare le impostazioni di efficienza della destinazione	648
Crea pianificazioni SnapMirror e SnapVault	649
Creare relazioni a cascata o a fanout per estendere la protezione da una relazione di protezione esistente	650
Modificare le relazioni di protezione dalla pagina Relazioni volume	650
Modificare le relazioni di protezione dalla pagina Dettagli volume/salute	651
Creare una policy SnapMirror per massimizzare l'efficienza del trasferimento	652
Crea una policy SnapVault per massimizzare l'efficienza del trasferimento	652
Annulla un trasferimento di protezione dati attivo dalla pagina Relazioni volume	653
Annulla un trasferimento di protezione dati attivo dalla pagina dei dettagli Volume/Stato	654
Disattiva una relazione di protezione dalla pagina Relazioni di volume	654
Disattiva una relazione di protezione dalla pagina dei dettagli Volume/Salute	655
Interrompere una relazione SnapMirror dalla pagina Relazioni volume	656
Rimuovere una relazione di protezione dalla pagina Relazioni di volume	656
Riprendi i trasferimenti pianificati su una relazione sospesa dalla pagina Relazioni di volume	657
Riprendi i trasferimenti programmati su una relazione sospesa dalla pagina dei dettagli Volume/Salute	658
Inizializzare o aggiornare le relazioni di protezione dalla pagina Relazioni volume	658
Inizializza o aggiorna le relazioni di protezione dalla pagina dei dettagli Volume/Stato	659
Risincronizzare le relazioni di protezione dalla pagina Relazioni volume	660
Relazioni di protezione inversa dalla pagina Relazioni di volume	661
Ripristinare i dati utilizzando le pagine Volume e Dettagli volume/integrità	662
Quali sono i pool di risorse	663
Creare pool di risorse	664
Modifica pool di risorse	664
Visualizza l'inventario dei pool di risorse	665
Aggiungi membri al pool di risorse	665
Rimuovere gli aggregati dai pool di risorse	665
Elimina pool di risorse	666
Monitorare le relazioni di protezione del ripristino di emergenza della VM di archiviazione	666
Informazioni sulle associazioni delle VM di archiviazione	668
Requisiti SVM e pool di risorse per supportare i servizi di archiviazione	670
Quali sono i lavori	671
Monitorare i lavori	671
Visualizza i dettagli del lavoro	672
Interrompere i lavori	672
Riprova un processo di protezione non riuscito	673

Descrizione delle finestre e delle finestre di dialogo delle relazioni di protezione	673
Genera report personalizzati	716
Reporting del gestore unificato	716
Punti di accesso per la generazione di report	716
Comprendere i report	718
Comprendere la relazione tra vista e report	718
Tipi di report	719
Limitazioni alla segnalazione	721
Lavorare con i report	721
Flusso di lavoro del report	721
Avvio rapido della segnalazione	722
Cerca un report programmato	725
Personalizza i report	725
Scarica i report	729
Pianifica i report	729
Pianifica un rapporto	729
Gestire le pianificazioni dei report	732
Esempi di report personalizzati	734
Personalizza i report di archiviazione del cluster	735
Personalizza i report sulla capacità aggregata	738
Personalizza i report sulla capacità del volume	740
Personalizza i report sulla capacità di Qtree	743
Personalizza i report di condivisione NFS	744
Personalizza i report delle VM di archiviazione	745
Personalizza i report sulle relazioni di volume	747
Personalizza i report sulle prestazioni del volume	751
Esempi di report di Microsoft Excel	752
Crea un report per mostrare una tabella e un grafico della capacità aggregata	752
Crea un report per mostrare grafici aggregati della capacità totale rispetto a quella disponibile	754
Crea un report per visualizzare i grafici della capacità del volume disponibile	758
Crea un report per visualizzare gli aggregati che hanno il maggior numero di IOPS disponibili	760
Gestire l'archiviazione utilizzando le API REST	763
Inizia con le API REST Active IQ Unified Manager	763
Pubblico per questo contenuto	763
Accesso e categorie API Active IQ Unified Manager	763
Servizi REST offerti in Active IQ Unified Manager	765
Versione API in Active IQ Unified Manager	765
Risorse di archiviazione in ONTAP	766
Accesso e autenticazione API REST in Active IQ Unified Manager	767
Autenticazione	769
Codici di stato HTTP utilizzati in Active IQ Unified Manager	770
Consigli per l'utilizzo delle API per Active IQ Unified Manager	771
Registri per la risoluzione dei problemi	771
Processi asincroni degli oggetti di lavoro	772
Ciao server API	773

API REST di Unified Manager	777
Gestire gli oggetti di archiviazione in un data center utilizzando le API	778
Accedi alle API ONTAP tramite accesso proxy	785
Eseguire attività amministrative utilizzando le API	788
Gestisci gli utenti tramite API	789
Visualizza le metriche delle prestazioni utilizzando le API	790
Visualizza i lavori e i dettagli del sistema	800
Gestisci eventi e avvisi tramite API	801
Gestisci i carichi di lavoro utilizzando le API	804
Flussi di lavoro API comuni per la gestione dell'archiviazione	813
Comprendere le chiamate API utilizzate nei flussi di lavoro	813
Determinare i problemi di spazio negli aggregati utilizzando le API	814
Determinare i problemi negli oggetti di archiviazione utilizzando le API degli eventi	815
Risolvere i problemi dei volumi ONTAP utilizzando le API del gateway	816
Flussi di lavoro API per la gestione del carico di lavoro	820
Note legali	848
Copyright	848
Marchi	848
Brevetti	848
Politica sulla riservatezza	848
Open source	848

Documentazione Active IQ Unified Manager

Note di rilascio

Fornisce un riepilogo delle nuove funzionalità, delle limitazioni e dei problemi noti di Active IQ Unified Manager 9.16.

Per maggiori informazioni, vedere il ["Note sulla versione Active IQ Unified Manager"](#) .

Iniziare

Istruzioni di avvio rapido per le installazioni VMware

Puoi scaricare il `.tar` file che contiene un certificato radice, un README file e un OVA file e distribuire Unified Manager come appliance virtuale.

Requisiti di sistema

- Sistema operativo: VMware ESXi 8.0
- RAM: 12 GB
- CPU: 9572 MHz totali
- Spazio libero su disco: 5 GB (thin provisioning), 152 GB (thick provisioning)

Per i requisiti di sistema dettagliati, vedere ["Requisiti per l'installazione di Unified Manager"](#) E ["Matrice di interoperabilità"](#).

Installa Active IQ Unified Manager

Scarica il programma di installazione

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

Verificare l'integrità

È possibile verificare l'integrità del OVA file seguendo i passaggi forniti nel README file.

Installa Unified Manager

1. Nel vSphere Client, fare clic su **File > Distribuisci modello OVF**.
2. Individuare il file OVA e utilizzare la procedura guidata per distribuire l'appliance virtuale sul server ESXi.
3. Nella pagina Dettagli revisione, nella sezione Editore, il messaggio Entrust Code Signing - OVCS2 (Trusted certificate) conferma l'integrità del file scaricato OVA file. Per il messaggio Entrust Code Signing - OVCS2 (Invalid certificate), aggiornare VMware vCenter Server alla versione 7.0U3E o successiva.
4. Nella pagina Personalizza modello, nella scheda Proprietà, compilare i campi come richiesto per il tipo di installazione che si sta eseguendo:
 - Per la configurazione statica, immettere le informazioni richieste in tutti i campi. Non è obbligatorio aggiungere informazioni per il campo **DNS secondario**.
 - Per DHCP che utilizza IPv4, non aggiungere alcuna informazione in nessun campo.
 - Per DHCP che utilizza IPv6, selezionare la casella "Abilita indirizzamento IPv6 automatico". Non aggiungere alcuna informazione in nessun altro campo.

5. Accendere la macchina virtuale.
6. Fare clic sulla scheda Console per visualizzare il processo di avvio iniziale.
7. Configura 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 connettersi all'interfaccia utente Web di Unified Manager.

Istruzioni rapide per l'installazione di Linux

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

Requisiti di sistema

- Sistema operativo: Red Hat Enterprise Linux versioni 8.x e 9.4, basate sull'architettura x86_64, installate utilizzando l'ambiente di base "Server con GUI" dall'opzione **Selezione software** del programma di installazione del sistema operativo
- RAM: 12 GB, CPU: 9572 MHz totali
- Spazio libero su disco: 100 GB di spazio su disco nel /opt/netapp/data directory, 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 ha 10 GB di spazio libero.

Per i requisiti di sistema dettagliati e per informazioni sull'installazione del prodotto in un sito protetto, vedere ["Requisiti per l'installazione di Unified Manager"](#) e il ["Matrice di interoperabilità"](#).

Installa Active IQ Unified Manager

Scarica il programma di installazione

1. Scarica il `ActiveIQUnifiedManager-<version>.zip` pacchetto di installazione insieme al certificato di firma del codice(`.pem`) e firma digitale(`.sig`).
2. Nella directory in cui hai scaricato il file di installazione, esegui:

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

Verificare l'integrità

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

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

Verifica la configurazione del repository

Le procedure per la configurazione di un repository Red Hat Enterprise Linux sono specifiche del sito. Puoi usare il `pre_install_check.sh` script incluso nel pacchetto di installazione per verificare la configurazione del sistema operativo. Se il sistema è connesso a Internet, si ricevono automaticamente le istruzioni per configurare il repository Red Hat Enterprise Linux.

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

Installa Unified Manager

Unified Manager utilizza il `yum` utilità per installare il software e qualsiasi software dipendente. Poiché esistono diverse immagini di Red Hat Enterprise Linux, i pacchetti installati dipendono dal software presente nelle immagini. IL `yum` L'utilità determina i pacchetti software dipendenti per l'installazione. Se hai bisogno di maggiori informazioni sui pacchetti software dipendenti, consulta il "[Requisiti di installazione e software Linux](#)".

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
```

O

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

Al termine dell'installazione vengono visualizzate le informazioni per connettersi all'interfaccia utente Web di Unified Manager. Se non riesci a connetterti all'interfaccia utente Web, fai riferimento a `README` file allegato al software per maggiori 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 relativi a capacità di archiviazione dei dati, disponibilità, prestazioni e protezione.

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 sul sistema operativo Windows a 64 bit per le seguenti lingue:

- Inglese
- giapponese
- cinese semplificato
- RAM: 12 GB
- CPU: 9572 MHz totali
- 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 i requisiti di sistema dettagliati, vedere ["Requisiti per l'installazione di Unified Manager"](#) E ["Matrice di interoperabilità"](#) .

Installa Active IQ Unified Manager

Scarica il programma di installazione

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

Installa Unified Manager

Per installare Unified Manager, assicurati di avere installato Microsoft .NET 4.5.2 o una versione successiva. Come parte del processo di installazione, Unified Manager installa altri pacchetti di terze parti, se necessario. Per ulteriori informazioni sui pacchetti software dipendenti, fare riferimento a ["Requisiti di installazione e software Windows"](#) .

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

Installa Unified Manager sui sistemi VMware vSphere

Introduzione ad Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) consente di monitorare e gestire lo stato e le prestazioni dei sistemi di archiviazione ONTAP da un'unica interfaccia. È possibile distribuire Unified Manager su un server Linux, su un server Windows o come appliance virtuale su un host VMware.

Dopo aver completato l'installazione e aver aggiunto i cluster che si desidera gestire, Unified Manager fornisce un'interfaccia grafica che visualizza la capacità, la disponibilità, la protezione e lo stato delle prestazioni dei sistemi di storage monitorati.

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Cosa fa il server Unified Manager

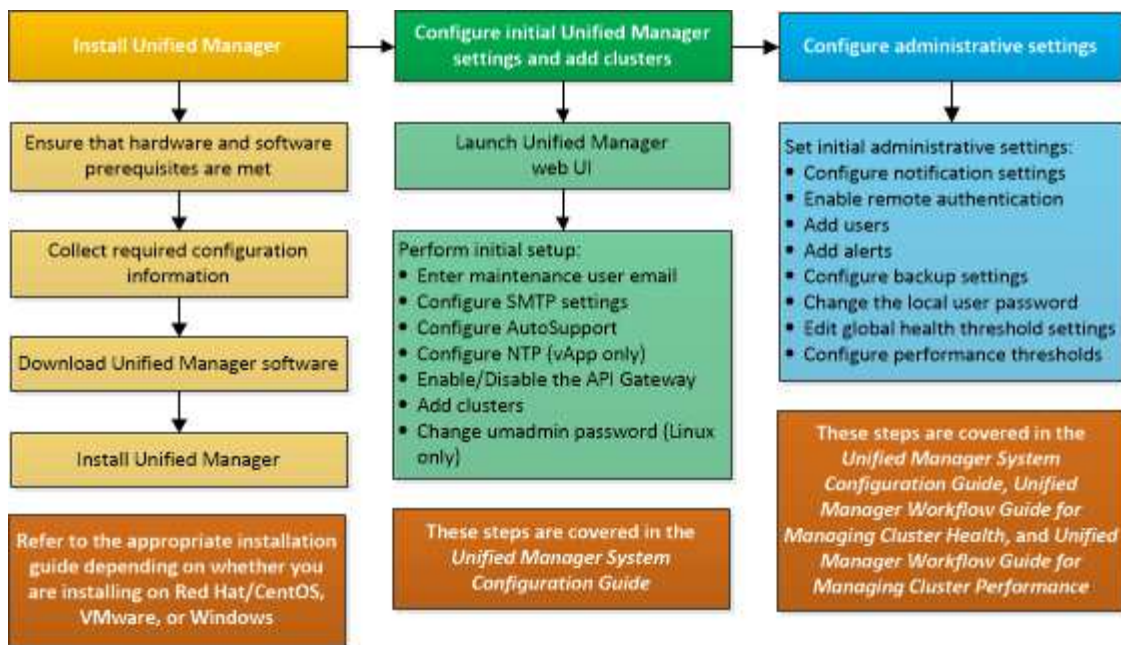
L'infrastruttura del server Unified Manager è composta da un'unità di raccolta dati, un database e un server applicativo. Fornisce servizi infrastrutturali quali individuazione, monitoraggio, controllo degli accessi basato sui ruoli (RBAC), auditing e registrazione.

Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare se ci sono problemi nel cluster.

Panoramica della sequenza di installazione

Il flusso di lavoro di installazione descrive le attività che è necessario eseguire prima di poter utilizzare Unified Manager.

In queste sezioni vengono descritti ciascuno degli elementi mostrati nel flusso di lavoro riportato di seguito.



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 maggiori dettagli sull'applicazione delle misure di sicurezza al server Unified Manager, consultare l'articolo della Knowledge Base.

["Supporto per misure di sicurezza applicate ad Active IQ Unified Manager per Clustered Data ONTAP"](#)

Informazioni correlate

Per maggiori informazioni, vedere ["Strumento matrice di interoperabilità NetApp"](#)

Requisiti di sistema hardware e infrastruttura virtuale

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.

Nella tabella seguente sono riportati 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 prestazioni accettabili.

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

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

Unified Manager può essere installato su sistemi con una piccola quantità di memoria, ma i 12 GB di RAM consigliati garantiscono che sia disponibile memoria sufficiente per prestazioni ottimali e che il sistema possa ospitare cluster e oggetti di archiviazione aggiuntivi man mano che la configurazione cresce. Non dovresti impostare limiti di memoria sulla VM in cui è distribuito Unified Manager e non dovresti abilitare funzionalità (ad esempio, il ballooning) che impediscono al software di utilizzare la memoria allocata sul 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 maggiori informazioni, vedere ["Guida alle migliori pratiche di Unified Manager"](#).

Lo scambio di pagine di memoria ha un impatto negativo sulle prestazioni del sistema e dell'applicazione di gestione. La competizione per risorse della CPU non disponibili a causa dell'utilizzo complessivo dell'host può compromettere le prestazioni.

Requisito per uso 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 prestazioni di Unified Manager.

Requisiti di spazio per i backup

Se si prevede di utilizzare la funzionalità di backup e ripristino di Unified Manager, allocare capacità aggiuntiva in modo che la directory o il disco "data" disponga di 150 GB di spazio. Un backup può essere scritto su una destinazione locale o su una destinazione remota. La procedura consigliata è quella di identificare una posizione remota esterna al sistema host di Unified Manager che disponga di 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 tale da poterlo utilizzare correttamente ping il nome host dall'host stesso. In caso di configurazione IPv6, è necessario verificare che ping6 al nome host ha esito positivo per garantire la corretta installazione di Unified Manager.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web del prodotto. Se hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, hai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, dovresti ottenere il nome host dal DNS.

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

Requisiti software e di installazione VMware

Il sistema VMware vSphere su cui si installa Unified Manager richiede una versione specifica del sistema operativo e versioni specifiche del software di supporto.

Software del sistema operativo

Il sistema operativo supportato è VMware ESXi 8.0.



Unified Manager OVA sui sistemi VMware vSphere esegue internamente Debian OS 12 (bookworm). 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 7.0 e 8.0

Per l'elenco completo e più aggiornato delle versioni ESXi supportate, consultare la matrice di interoperabilità.

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

Affinché l'appliance virtuale funzioni correttamente, l'ora del server VMware ESXi deve essere la stessa dell'ora del server NTP. La sincronizzazione dell'ora del server VMware ESXi con l'ora del server NTP previene errori di orario.

Requisiti di installazione

È supportato VMware High Availability per l'appliance virtuale Unified Manager.

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

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



Durante l'installazione o l'aggiornamento di Unified Manager, il software di terze parti e le patch di sicurezza 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 installare o aggiornare autonomamente 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 dei browser supportate.

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

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

Se si prevede di 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 dall'IdP.

Requisiti di protocollo e porta

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

Connessioni al server Unified Manager

Nelle installazioni tipiche non è necessario specificare i numeri di porta quando ci si connette all'interfaccia utente Web di Unified Manager, perché vengono sempre utilizzate le porte predefinite. Ad esempio, poiché Unified Manager tenta sempre di essere eseguito sulla sua 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
Interfaccia utente web di Unified Manager	HTTP	80	Utilizzato per accedere all'interfaccia utente Web di Unified Manager; reindirizza automaticamente alla porta protetta 443.
Interfaccia utente Web di Unified Manager e 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 tramite HTTPS.
Console di manutenzione	SSH/SFTP	22	Utilizzato per accedere alla console di manutenzione e recuperare i pacchetti di supporto.
Riga di comando di Linux	SSH/SFTP	22	Utilizzato per accedere alla riga di comando di Red Hat Enterprise Linux e recuperare i bundle di supporto.
Registro di sistema	UDP	514	Utilizzato per accedere ai messaggi EMS basati su abbonamento dai sistemi ONTAP e per creare eventi basati sui messaggi.

Interfaccia	Protocollo	Porta	Descrizione
RIPOSO	HTTPS	9443	Utilizzato per accedere in tempo reale agli eventi EMS basati su REST API dai sistemi ONTAP autenticati.
database MySQL	MySQL	3306	Utilizzato per abilitare l'accesso di OnCommand Workflow Automation e OnCommand API Services a Unified Manager.
Broker AMQP QPID	TCP/IP	56072	Utilizzato per la comunicazione di messaggi interni.
Broker AMQP QPID	WebSocket su TCP	56080	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud).
Broker AMQP QPID	WebSocket su TCP	56443	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud). La comunicazione tramite questa porta supporta la crittografia fornita da TLS o SSL.



La porta predefinita per MySQL, 3306, è limitata solo a localhost durante l'installazione di Unified Manager sui sistemi VMware vSphere. Ciò non ha alcun impatto sugli scenari 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 opzione sulla console di manutenzione. Per informazioni, vedere ["Opzioni di menu aggiuntive"](#). Le porte utilizzate per la comunicazione HTTP e HTTPS (porte 80 e 443) possono essere modificate tramite la console di manutenzione di Unified Manager. Per maggiori informazioni, vedere ["Menu della console di manutenzione"](#).

Connessioni dal server Unified Manager

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

A seconda dell'ambiente, 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 tramite i seguenti protocolli e porte ai sistemi di archiviazione gestiti, ai server e ad altri componenti:

Destinazione	Protocollo	Porta	Descrizione
Sistema di archiviazione	HTTPS	443/TCP	Utilizzato per monitorare e gestire i sistemi di archiviazione.  Se si utilizza questa porta o qualsiasi altra porta per connettersi al server VMware vCenter o ESXi, assicurarsi che la porta sia disponibile e possa essere connessa in un sito protetto.
Sistema di archiviazione	NDMP	10000/TCP	Utilizzato per determinate operazioni di ripristino Snapshot.
Server AutoSupport	HTTPS	443	Utilizzato per inviare informazioni AutoSupport . Per eseguire questa funzione è necessario l'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

Destinazione	Protocollo	Porta	Descrizione
SMTP	25	Utilizzato per inviare e-mail di notifica di avviso.	Mittente trap SNMP
SNMPv1 o SNMPv3	162/UDP	Utilizzato per inviare trap SNMP di notifica di avviso.	Server fornitore di dati esterno
TCP	2003	Utilizzato per inviare dati sulle prestazioni a un fornitore di dati esterno, come Graphite.	server NTP
NTP	123/UDP	Utilizzato per sincronizzare l'ora sul server Unified Manager con un server orario NTP esterno. (Solo sistemi VMware)	Registro di sistema

Completa il foglio di lavoro

Prima di installare e configurare Unified Manager, è necessario avere a portata di mano informazioni specifiche sul proprio ambiente. 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 distribuito il software	Il tuo valore
Indirizzo IP del server ESXi	
Ospita un nome di dominio completamente qualificato	
Indirizzo IP dell'host	
Maschera di rete	
Indirizzo IP del gateway	
Indirizzo DNS primario	
Indirizzo DNS secondario	
Cerca domini	

Sistema su cui viene distribuito il software	Il tuo valore
Nome utente di manutenzione	
Password utente di manutenzione	

Informazioni sulla configurazione di Unified Manager

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

Collocamento	Il tuo valore
Indirizzo email dell'utente addetto alla manutenzione	
server NTP	
Nome host o indirizzo IP del server SMTP	
Nome utente SMTP	
password SMTP	
porta SMTP	25 (valore predefinito)
Email 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 di binding LDAP	
Password di Active Directory o password di binding LDAP	
Nome distinto di base del server di autenticazione	
URL del provider di identità (IdP)	
Metadati del provider di identità (IdP)	
Indirizzi IP dell'host di destinazione della trappola SNMP	
porta SNMP	

Informazioni sul cluster

I dettagli sui sistemi di archiviazione gestiti tramite Unified Manager.

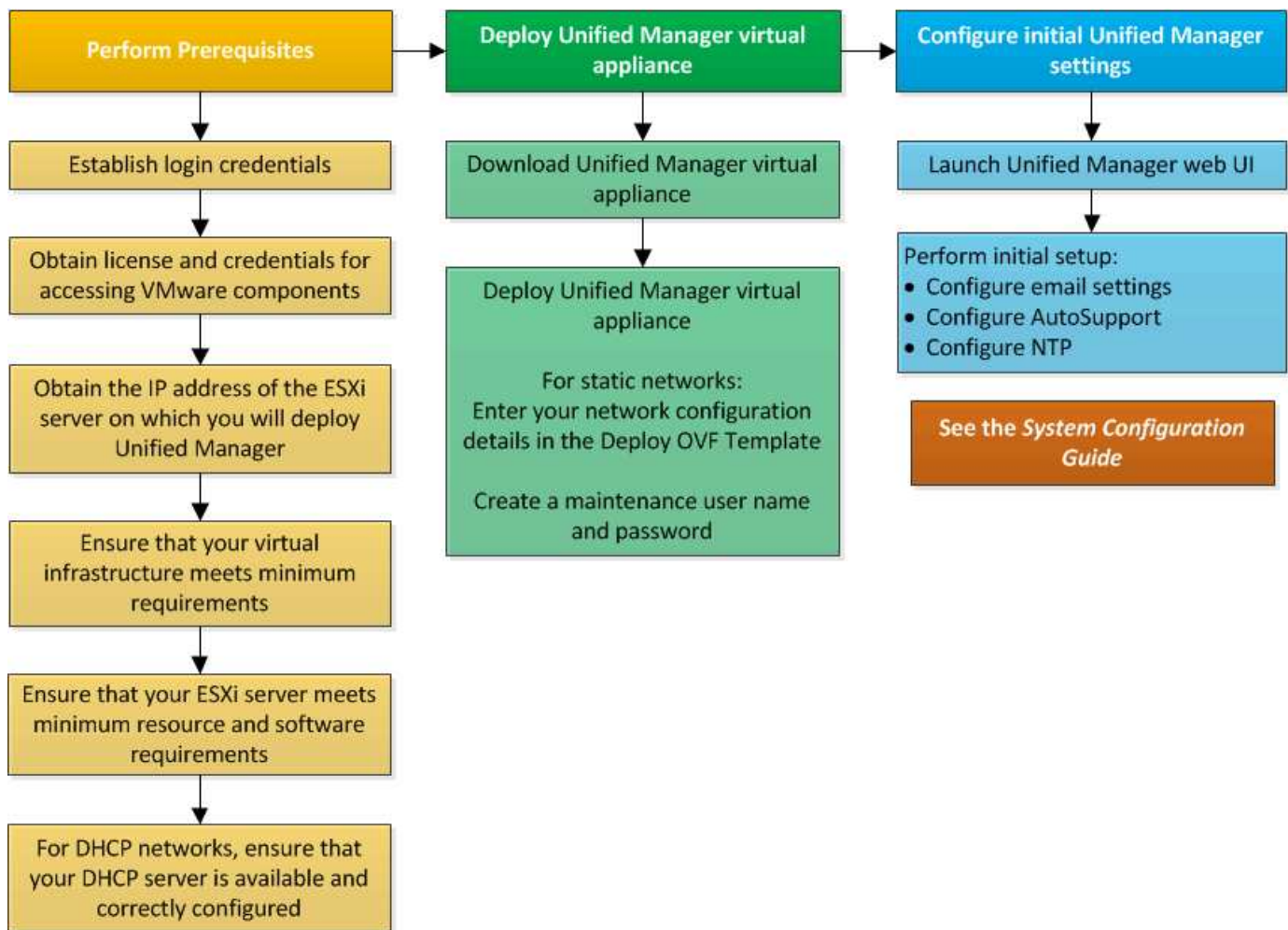
Cluster 1 di N	Il tuo valore
Nome host o indirizzo IP di gestione del cluster	
Nome utente dell'amministratore ONTAP  All'amministratore deve essere stato assegnato il ruolo "admin".	
Password amministratore ONTAP	
Protocollo	HTTPS

Installa, aggiorna e rimuovi il software Unified Manager

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

Panoramica del processo di distribuzione

Il flusso di lavoro di distribuzione descrive le attività che è necessario eseguire prima di poter utilizzare Unified Manager.



Distribuisce 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 per la manutenzione e l'esecuzione della configurazione iniziale nell'interfaccia utente Web.

Prima di iniziare

- È necessario verificare e completare i requisiti di sistema per la distribuzione.

Vedere "[Requisiti di sistema](#)".

- Assicurati di avere le seguenti informazioni:
 - Credenziali di accesso per il sito di supporto NetApp
 - Credenziali per l'accesso a VMware vCenter Server e vSphere Web Client
 - Indirizzo IP del server ESXi su cui si sta distribuendo l'appliance virtuale Unified Manager
 - Dettagli sul data center, come lo spazio di archiviazione nel datastore e i requisiti di memoria
 - Se si prevede di utilizzare l'indirizzamento IPv6, è necessario abilitare IPv6 sull'host.

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

Dovresti accedere alla console di manutenzione tramite la console VMware e non tramite SSH.



A partire da Unified Manager 9.8, VMware Tools è stato sostituito da 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.

Dopo aver completato la distribuzione e la configurazione iniziale, è possibile aggiungere cluster o configurare impostazioni di rete aggiuntive nella console di manutenzione, quindi accedere all'interfaccia utente Web.

Passi

1. Segui i passaggi in ["Scarica Unified Manager"](#).
2. Inoltre, seguire i passaggi in ["Distribuisci l'appliance virtuale Unified Manager"](#).

Scarica il file di installazione di Unified Manager

Scaricare il file di installazione di Unified Manager dal sito di supporto NetApp per distribuire Unified Manager come appliance virtuale.

Prima di iniziare

Dovresti avere le credenziali di accesso per il sito di supporto NetApp.

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

Passi

1. Accedi al sito di supporto NetApp e vai alla pagina di download per 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. Scarica e salva il `.tar` file per l'installazione di VMware vSphere in una directory locale o di rete accessibile al tuo vSphere Client.
4. Verificare il checksum per assicurarsi che il software sia stato scaricato correttamente.
5. Passare alla directory in cui è stato scaricato il `.tar` file e inserisci il seguente comando nella finestra del terminale per espandere il bundle Unified Manager:

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

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

6. Verificare l'integrità del `OVA` file seguendo i passaggi forniti nel `README` file.

Distribuisci l'appliance virtuale Unified Manager

Dopo aver scaricato il file di installazione, distribuisci Unified Manager come appliance virtuale. Utilizzare vSphere Web Client per distribuire l'appliance virtuale su un server

ESXi. Quando si distribuisce l'appliance virtuale, viene creata una macchina virtuale.

Prima di iniziare

Dovresti rivedere i requisiti di sistema. Apportare le modifiche necessarie prima di distribuire l'appliance virtuale Unified Manager.

Vedere ["Requisiti dell'infrastruttura virtuale"](#) .

Vedere ["Requisiti software e di installazione VMware"](#) .

Se si utilizza il protocollo DHCP (Dynamic Host Configuration Protocol), assicurarsi che il server DHCP sia disponibile e che le configurazioni DHCP e della scheda di rete della macchina virtuale (VM) 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 subnet e che siano state configurate le voci appropriate del server DNS.

Prima di distribuire l'appliance virtuale, procurarsi le seguenti informazioni:

- Credenziali per l'accesso a VMware vCenter Server e vSphere Web Client
- Indirizzo IP del server ESXi su cui si sta distribuendo l'appliance virtuale Unified Manager
- Dettagli sul data center, come la disponibilità di spazio di archiviazione
- Se non si utilizza DHCP, ottenere gli indirizzi IPv4 o IPv6 per i dispositivi di rete a cui si intende connettersi:
 - Nome di dominio completo (FQDN) 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 da 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 viene distribuito l'appliance virtuale, 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.

È supportato VMware High Availability per l'appliance virtuale Unified Manager.

Passi

1. Nel vSphere Client, fare clic su **File > Distribuisci modello OVF**.
2. Completare la procedura guidata Distribuisci modello OVF per distribuire l'appliance virtuale Unified Manager.

Nella pagina Dettagli della recensione:

- Verificare i dettagli della sezione Editore. Il messaggio **Entrust Code Signing - OVCS2 (Certificato attendibile)** conferma l'integrità del certificato scaricato OVA file. + Se viene visualizzato il messaggio **Entrust Code Signing - OVCS2 (certificato non valido)**, aggiornare VMware vCenter Server alla

versione 7.0U3E o successiva.

Nella pagina Personalizza modello:

- Lasciare tutti i campi vuoti quando si utilizza DHCP e l'indirizzamento IPv4.
 - Selezionare la casella "Abilita indirizzamento IPv6 automatico" e lasciare vuoti tutti gli altri campi quando si utilizza DHCP e l'indirizzamento IPv6.
 - Se si desidera utilizzare una configurazione di rete statica, è possibile compilare i campi in questa pagina e queste impostazioni verranno applicate durante la distribuzione. 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 distribuito l'appliance virtuale Unified Manager sul server ESXi, accendere la VM facendo clic con il pulsante destro del mouse sulla VM e selezionando **Accendi**.



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

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

Il processo di avvio iniziale richiede alcuni minuti.

5. Per configurare il fuso orario, inserisci la tua area geografica e la tua città o regione come richiesto nella finestra della console VM.

Tutte le informazioni sulla data visualizzate utilizzano il fuso orario configurato per Unified Manager, indipendentemente dall'impostazione del fuso orario sui dispositivi gestiti. Se i sistemi di archiviazione e il server di gestione sono configurati con lo stesso server NTP, fanno riferimento allo stesso istante di tempo, anche se appaiono in modo diverso. Ad esempio, se si crea una copia Snapshot utilizzando un dispositivo configurato con un fuso orario diverso da quello del server di gestione, il timestamp sarà l'ora del server di gestione.

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

Se usi...	Allora fai così...
DHCP	Selezionare Riprova DHCP. Se si prevede di utilizzare DHCP, è necessario assicurarsi che sia configurato correttamente. Se si utilizza una rete abilitata DHCP, le voci del server FQDN e 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 sicurezza. Se non hai configurato una rete abilitata DHCP, devi immettere manualmente le informazioni di configurazione della rete.

Se usi...	Allora fai così...
Una configurazione di rete statica	a. Selezionare Inserisci i dettagli per la configurazione di rete statica. Il processo di configurazione richiede alcuni minuti. b. Conferma i valori immessi e seleziona Y.

7. Al prompt, immettere un nome utente di manutenzione, quindi fare clic su **Invio**.

Il nome utente addetto alla manutenzione deve iniziare con una lettera dalla a alla z, seguita da una qualsiasi combinazione di -, az o 0-9.

8. Al prompt, immettere una password, quindi fare clic su **Invio**.

La console della VM visualizza l'URL per l'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](#)".

Aggiorna Unified Manager

È possibile aggiornare Active IQ Unified Manager alla versione 9.16 solo dalla versione 9.13 o 9.14.

Durante il processo di aggiornamento, Unified Manager non è disponibile. Prima di aggiornare 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 disconnettere i due prodotti e quindi configurare una nuova connessione Workflow Automation dopo aver eseguito gli aggiornamenti. Se si esegue l'aggiornamento solo a uno dei prodotti, è necessario accedere a Workflow Automation dopo l'aggiornamento e verificare che stia ancora acquisendo dati da Unified Manager.

Passi

1. Segui i passaggi in "[Scarica l'immagine ISO di Unified Manager](#)".
2. Inoltre, seguire i passaggi descritti 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 ogni versione.

Non tutte le versioni di Unified Manager possono eseguire un aggiornamento sul posto alle versioni successive. Gli aggiornamenti di Unified Manager sono limitati al modello N-2, il che significa che un aggiornamento può essere eseguito solo entro le prossime 2 release su tutte le piattaforme. Ad esempio, è possibile eseguire un aggiornamento a Unified Manager 9.16 solo da Unified Manager 9.13 e 9.14.

Se si utilizza una versione precedente a quelle supportate, sarà necessario prima aggiornare l'istanza di Unified Manager a una delle versioni supportate e poi alla versione corrente.

Ad esempio, se la versione installata è Unified Manager 9.9 e si desidera eseguire l'aggiornamento a Unified Manager 9.14, è necessario seguire una sequenza di aggiornamenti.

Esempio di percorso di aggiornamento:

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

Per ulteriori informazioni sulla matrice del percorso di aggiornamento, vedere questo ["articolo della knowledge base \(KB\)"](#) .

Scarica il file di aggiornamento di Unified Manager

Prima di aggiornare Unified Manager, scaricare il file di aggiornamento di Unified Manager dal sito di supporto NetApp .

Prima di iniziare

Dovresti avere le credenziali di accesso al sito di supporto NetApp .

Passi

1. Accedi al sito di supporto NetApp :

["Sito di supporto NetApp"](#)

2. Vai alla pagina Download per aggiornare Unified Manager su VMware vSphere.
3. Scarica il .iso immagine per l'aggiornamento e salvarla in una directory locale o di rete accessibile al tuo vSphere Client.
4. Verificare il checksum per assicurarsi che il software sia stato scaricato correttamente.

Aggiorna l'appliance virtuale Unified Manager

È possibile aggiornare l'appliance virtuale Active IQ Unified Manager dalle versioni 9.13 o 9.14 alla versione 9.16.

Prima di iniziare

Assicurarsi che:

- Hai scaricato il file di aggiornamento, l'immagine ISO dal sito di supporto NetApp .
- Il sistema su cui si sta aggiornando Unified Manager soddisfa i requisiti di sistema e software.

Vedere ["Requisiti dell'infrastruttura virtuale"](#) .

Vedere ["Requisiti software e di installazione VMware"](#) .

- Per gli utenti di vSphere 6.5 e versioni successive, è stata installata VMware Remote Console (VMRC).
- Durante l'aggiornamento, potrebbe esserti richiesto di confermare se desideri mantenere le impostazioni predefinite precedenti per la conservazione dei dati sulle prestazioni per 13 mesi o modificarle in 6 mesi. Dopo la conferma, i dati storici sulle prestazioni vengono eliminati dopo 6 mesi.

- Hai le seguenti informazioni:
 - Credenziali di accesso per il sito di supporto NetApp
 - Credenziali per l'accesso a VMware vCenter Server e vSphere Web Client
 - Credenziali per l'utente addetto alla manutenzione di Unified Manager

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

Se hai associato Workflow Automation e Unified Manager, devi aggiornare manualmente il nome host in Workflow Automation.

Passi

1. In vSphere Client, fare clic su **Home > Inventario > VM e modelli**.
2. Selezionare la macchina virtuale (VM) su cui è installato l'appliance virtuale Unified Manager.
3. Se la VM Unified Manager è in esecuzione, accedere a **Riepilogo > Comandi > Arresta Guest**.
4. Creare una copia di backup, ad esempio uno snapshot o un clone, della VM di Unified Manager per creare un backup coerente con l'applicazione.
5. Da vSphere Client, accendere la VM Unified Manager.
6. Avviare VMware Remote Console.
7. Fare clic sull'icona **CDROM** e selezionare **Connetti al file immagine disco (.iso)**.
8. Seleziona il `ActiveIQUnifiedManager-<version>-virtual-update.iso` file e fare clic su **Apri**.
9. Fare clic sulla scheda **Console**.
10. Accedi alla console di manutenzione di Unified Manager.
11. Nel menu principale, seleziona **Aggiorna**.

Viene visualizzato un messaggio che informa che Unified Manager non sarà disponibile durante il processo di aggiornamento e che verrà ripreso al termine.

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 completamento del processo di aggiornamento e del riavvio dei servizi di Unified Manager può richiedere diversi minuti.

14. Premere un tasto qualsiasi per continuare.

Verrai automaticamente disconnesso dalla console di manutenzione.

15. **Facoltativo:** accedi alla console di manutenzione e verifica 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. Tieni presente che è necessario attendere il completamento del processo di individuazione prima di eseguire qualsiasi attività nell'interfaccia utente.

Riavviare la macchina virtuale Unified Manager

È possibile riavviare la macchina virtuale (VM) di Unified Manager dalla console di manutenzione. Dopo aver generato un nuovo certificato di sicurezza o se si verifica un problema con la VM, è necessario riavviarla.

Prima di iniziare

- L'appliance virtuale deve essere accesa.
- È necessario aver effettuato l'accesso alla console di manutenzione di Unified Manager come utente addetto alla manutenzione.

È anche possibile riavviare la macchina virtuale da vSphere utilizzando l'opzione VMware **Riavvia Guest**. Fare riferimento a ["il cmdlet Restart-VMGuest nel riferimento ai CMDLET VMware vSphere PowerCLI di Broadcom."](#)

Passi

1. Nella console di manutenzione, selezionare **Configurazione di sistema > Riavvia macchina virtuale**.
2. Avvia l'interfaccia utente Web di Unified Manager dal tuo browser ed effettua l'accesso.

Rimuovi Unified Manager

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

Prima di iniziare

- È necessario disporre delle credenziali per accedere a VMware vCenter Server e vSphere Web Client.
- Qualsiasi connessione attiva del server Unified Manager a un server Workflow Automation deve essere chiusa.
- Tutti i cluster (origini dati) devono essere rimossi dal server Unified Manager prima di rimuovere la macchina virtuale (VM).

Passi

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 > Inventario > VM e modelli**.
3. Selezionare la VM che si desidera rimuovere e fare clic sulla scheda **Riepilogo**.
4. Se la VM è in esecuzione, fare clic su **Alimentazione > Arresta Guest**.
5. Fare clic con il pulsante destro del mouse sulla VM che si desidera rimuovere e fare clic su **Elimina dal disco**.

Installa Unified Manager sui sistemi Linux

Introduzione ad Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) consente di monitorare e gestire lo stato e le prestazioni dei sistemi di archiviazione ONTAP da un'unica interfaccia. È possibile distribuire Unified Manager su un server Linux, su un server Windows o come appliance virtuale (vApp) su un host VMware.

Dopo aver completato l'installazione e aver aggiunto i cluster che si desidera gestire, Unified Manager fornisce un'interfaccia grafica che visualizza la capacità, la disponibilità, la protezione e lo stato delle prestazioni dei sistemi di storage monitorati.

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Cosa fa il server Unified Manager

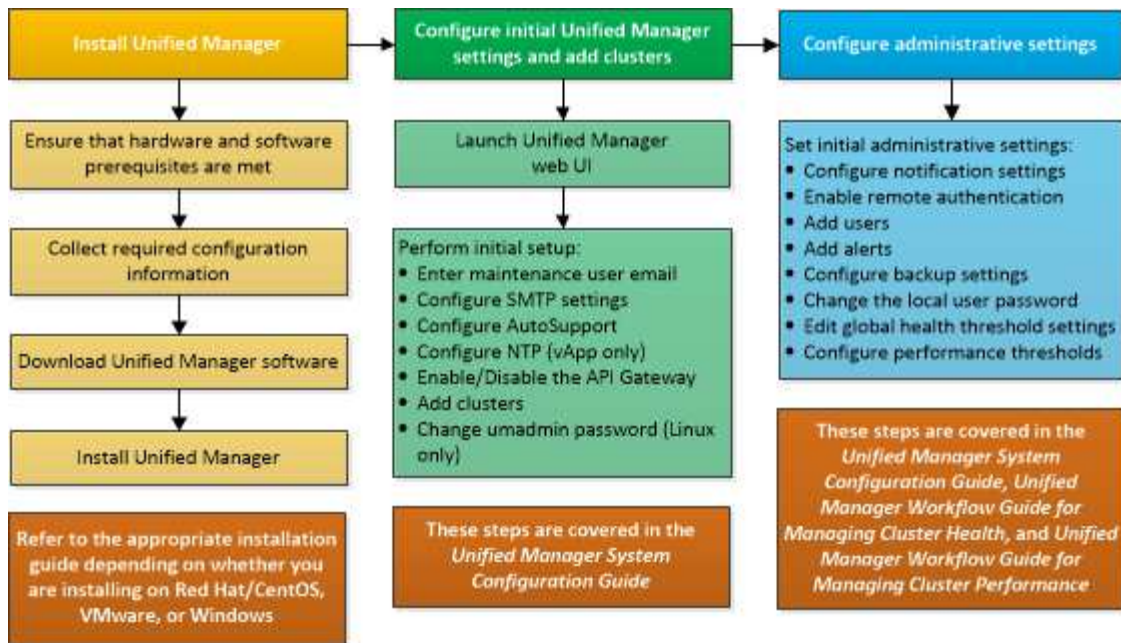
L'infrastruttura del server Unified Manager è composta da un'unità di raccolta dati, un database e un server applicativo. Fornisce servizi infrastrutturali quali individuazione, monitoraggio, controllo degli accessi basato sui ruoli (RBAC), auditing e registrazione.

Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare se ci sono problemi nel cluster.

Panoramica della sequenza di installazione

Il flusso di lavoro di installazione descrive le attività che è necessario eseguire prima di poter utilizzare Unified Manager.

In queste sezioni vengono descritti ciascuno degli elementi mostrati nel flusso di lavoro riportato di seguito.



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 maggiori dettagli sull'applicazione delle misure di sicurezza al server Unified Manager, consultare l'articolo della Knowledge Base.

["Supporto per misure di sicurezza applicate ad Active IQ Unified Manager per Clustered Data ONTAP"](#)

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Requisiti di sistema hardware e infrastruttura virtuale

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.

Nella tabella seguente sono riportati 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 prestazioni accettabili.

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

Configurazione hardware	Impostazioni consigliate
Capacità del ciclo della CPU	9572 MHz totali (requisito minimo 9572 MHz)
Spazio libero su disco	150 GB, dove la capacità è allocata come segue: • 50 GB assegnati alla partizione root • 100 GB di spazio libero su disco assegnato al <code>/opt/netapp/data</code> directory, che è montata su un'unità LVM o su un disco locale separato collegato al sistema di destinazione  Per montaggio separato <code>/opt</code> e <code>/var/log</code> directory, assicurarsi che <code>/opt</code> ha 15 GB e <code>/var/log</code> ha 16 GB di spazio libero. IL <code>/tmp</code> la directory dovrebbe avere 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 memoria sufficiente per prestazioni ottimali e che il sistema possa ospitare cluster e oggetti di archiviazione aggiuntivi man mano che la configurazione cresce. Non dovresti impostare limiti di memoria sulla VM in cui è distribuito Unified Manager e non dovresti abilitare funzionalità (ad esempio, il ballooning) che impediscono al software di utilizzare la memoria allocata sul 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, consultare la *Guida alle best practice*.

["Rapporto tecnico 4621: Guida alle best practice di Unified Manager"](#)

Lo scambio di pagine di memoria ha un impatto negativo sulle prestazioni del sistema e dell'applicazione di gestione. La competizione per risorse della CPU non disponibili a causa dell'utilizzo complessivo dell'host può compromettere le prestazioni.

Requisito per uso 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 prestazioni di Unified Manager.

Requisiti di spazio per i backup

Se si prevede di utilizzare la funzionalità di backup e ripristino di Unified Manager, allocare capacità aggiuntiva in modo che la directory o il disco "data" disponga di 150 GB di spazio. Un backup può essere scritto su una destinazione locale o su una destinazione remota. La procedura consigliata è quella di identificare una posizione remota esterna al sistema host di Unified Manager che disponga di 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 tale da poterlo utilizzare correttamente `ping` il nome host dall'host stesso. In caso di configurazione IPv6, è necessario

verificare che `ping6` al nome host ha esito positivo per garantire la corretta installazione di Unified Manager.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web del prodotto. Se hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, hai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, dovresti ottenere il nome host dal DNS.

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

Requisiti di installazione e software Linux

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 avere installate le seguenti versioni del sistema operativo e del software di supporto:

- Red Hat Enterprise Linux versioni 8.x e 9.4, basate sull'architettura x86_64.

Per l'elenco completo e più aggiornato delle versioni supportate di Red Hat Enterprise Linux, consultare la matrice di interoperabilità.

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

Il server dovrebbe essere dedicato all'esecuzione di Unified Manager. Non devono essere installate altre applicazioni sul server. È possibile che sul tuo sistema Linux sia installato uno scanner di vulnerabilità come Qualys a causa delle normative aziendali. Per evitare che l'installazione fallisca, è consigliabile disattivare lo scanner delle vulnerabilità prima di installare Unified Manager.



Gli scanner delle vulnerabilità (come Qualys) potrebbero comportare un elevato utilizzo della CPU durante la scansione della macchina virtuale (VM), sia internamente (quando Unified Manager e lo scanner delle vulnerabilità sono installati sulla stessa VM) sia esternamente (quando Unified Manager e lo scanner delle vulnerabilità sono installati su due server diversi e lo scanner delle vulnerabilità esegue la scansione della VM in cui è installato Unified Manager). Questo problema spesso impedisce alla VM di rispondere e influisce sui servizi di Unified Manager. Pertanto, NetApp consiglia di disabilitare lo scanner delle vulnerabilità nella VM in cui è installato Unified Manager. Se la disattivazione dello scanner non è un'opzione, eseguire la scansione della macchina virtuale al di fuori dell'orario lavorativo e riavviare i servizi al termine della scansione.

Software di terze parti

Unified Manager è distribuito su un server web WildFly. WildFly 26.1.3 è fornito in bundle e configurato con Unified Manager.

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

- MySQL Community Edition versione 8.4.4 (dal repository MySQL)
- OpenJDK versione 11.0.25 (dal repository Red Hat Extra Enterprise Linux Server)

- Python 3.9.x (dal repository di Red Hat Extra Enterprise Linux Server)
- 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 arrestare un'istanza in esecuzione di Unified Manager. 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.

Inoltre, l'installazione predefinita di Unified Manager include l'utente `umadmin` (utente di manutenzione predefinito) e l'utente `jboss` nei file `sudoers(ocum_sudoers E ocie_sudoers )` nel `/etc/sudoers.d/` elenco. Se rimuovi questo contenuto dal tuo ambiente a causa di policy di sicurezza o di uno strumento di monitoraggio della sicurezza, devi aggiungerlo di nuovo. È necessario conservare la configurazione `sudoers` perché alcune operazioni di Unified Manager richiedono questi privilegi `sudo`.

Requisiti di installazione

Di seguito sono elencate le best practice per l'installazione di Red Hat Enterprise Linux e dei repository associati sul sistema. I sistemi installati o configurati in modo diverso, oppure distribuiti fuori sede (nel cloud), potrebbero richiedere passaggi aggiuntivi e Unified Manager potrebbe non funzionare correttamente in tali distribuzioni.

- È necessario installare Red Hat Enterprise Linux secondo le best practice di Red Hat e selezionare le seguenti opzioni predefinite, che richiedono la selezione dell'ambiente di base "Server con GUI".
- Durante l'installazione di Unified Manager su Red Hat Enterprise Linux, 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 il `yum` Per trovare il software dipendente nei repository di Red Hat Enterprise Linux, è necessario 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, consultare la documentazione di Red Hat.

- Per installare correttamente le utilità di terze parti richieste sul sistema, è necessario abilitare il repository Extra Packages for Enterprise Linux (EPEL).

Se il repository EPEL non è configurato sul tuo sistema, devi scaricarlo e configurarlo manualmente.

Vedere ["Configurazione manuale del repository EPEL"](#) .

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

Se il repository MySQL non è configurato sul tuo sistema, devi scaricarlo e configurarlo manualmente.

Vedere ["Configurazione manuale del repository MySQL"](#) .

- È necessario installare una sola versione di Java sull'host Unified Manager; in caso contrario, il sistema potrebbe non essere in grado di determinare quale versione utilizzare. Vedere ["Dopo aver aggiornato Java sull'host Active IQ Unified Manager , i servizi non si avviano"](#) .

Se il sistema non ha accesso a Internet e i repository non vengono replicati da un sistema connesso a Internet a un sistema non connesso, è necessario seguire le istruzioni di installazione per determinare le dipendenze software esterne del sistema. Quindi puoi scaricare il software richiesto sul sistema connesso a Internet e copiare il `.rpm` file sul 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.



Non è consentito installare il software di terze parti richiesto da repository diversi da quelli elencati qui. Il software installato dai repository Red Hat è progettato espressamente per Red Hat Enterprise Linux ed è conforme alle best practice di Red Hat (layout delle directory, autorizzazioni e così via). Il software proveniente da altre posizioni potrebbe non seguire queste linee guida, il che potrebbe causare il fallimento dell'installazione di Unified Manager o problemi con gli aggiornamenti futuri.

Requisito della porta 443

Le immagini generiche di Red Hat Enterprise Linux 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 aver installato Unified Manager. L'esecuzione del seguente comando consente l'accesso alla porta 443 a tutti gli utenti esterni e alle applicazioni su un sistema operativo Red Hat Enterprise Linux generico.

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

È necessario installare Red Hat Enterprise Linux con l'ambiente di base "Server con GUI". Fornisce i comandi utilizzati nelle istruzioni di installazione di Unified Manager. Altri ambienti di base potrebbero richiedere l'installazione di comandi aggiuntivi per convalidare o completare l'installazione. Se il `firewall-cmd` non è disponibile sul tuo sistema, devi 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.



THP (Transparent Huge Pages) dovrebbe essere disabilitato sui sistemi Red Hat. Se abilitata, in alcuni casi può causare l'arresto di Unified Manager quando determinati processi consumano troppa 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 dei browser supportate.

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

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

Se si prevede di 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 dall'IdP.

Requisiti di protocollo e porta

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

Connessioni al server Unified Manager

Nelle installazioni tipiche non è necessario specificare i numeri di porta quando ci si connette all'interfaccia utente Web di Unified Manager, perché vengono sempre utilizzate le porte predefinite. Ad esempio, poiché Unified Manager tenta sempre di essere eseguito sulla sua 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
Interfaccia utente web di Unified Manager	HTTP	80	Utilizzato per accedere all'interfaccia utente Web di Unified Manager; reindirizza automaticamente alla porta protetta 443.
Interfaccia utente Web di Unified Manager e 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 tramite HTTPS.
Console di manutenzione	SSH/SFTP	22	Utilizzato per accedere alla console di manutenzione e recuperare i pacchetti di supporto.
Riga di comando di Linux	SSH/SFTP	22	Utilizzato per accedere alla riga di comando di Red Hat Enterprise Linux e recuperare i bundle di supporto.

Interfaccia	Protocollo	Porta	Descrizione
database MySQL	MySQL	3306	Utilizzato per abilitare l'accesso di OnCommand Workflow Automation e OnCommand API Services a Unified Manager.
Registro di sistema	UDP	514	Utilizzato per accedere ai messaggi EMS basati su abbonamento dai sistemi ONTAP e per creare eventi basati sui messaggi.
RIPOSO	HTTPS	9443	Utilizzato per accedere in tempo reale agli eventi EMS basati su REST API dai sistemi ONTAP autenticati.
database MySQL	MySQL	3306	Utilizzato per abilitare l'accesso di OnCommand Workflow Automation e OnCommand API Services a Unified Manager.
Broker AMQP QPID	TCP/IP	56072	Utilizzato per la comunicazione di messaggi interni.
Broker AMQP QPID	WebSocket su TCP	56080	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud).
Broker AMQP QPID	WebSocket su TCP	56443	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud). La comunicazione tramite questa porta supporta la crittografia fornita da TLS o SSL.



La porta predefinita per MySQL, 3306, è limitata solo a localhost durante l'installazione di Unified Manager sui sistemi Linux. Ciò non ha alcun impatto sugli scenari 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` opzione sulla console di manutenzione. Per informazioni, vedere ["Opzioni di menu aggiuntive"](#). Le porte utilizzate per la comunicazione HTTP e HTTPS (porte 80 e 443) possono essere modificate tramite la console di manutenzione di Unified Manager. Per maggiori informazioni, vedere ["Menu della console di manutenzione"](#).

Connessioni dal server Unified Manager

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

A seconda dell'ambiente, 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 tramite i seguenti protocolli e porte ai sistemi di archiviazione gestiti, ai server e ad altri componenti:

Destinazione	Protocollo	Porta	Descrizione
Sistema di archiviazione	HTTPS	443/TCP	Utilizzato per monitorare e gestire i sistemi di archiviazione.
Sistema di archiviazione	NDMP	10000/TCP	Utilizzato per determinate operazioni di ripristino Snapshot.
Server AutoSupport	HTTPS	443	Utilizzato per inviare informazioni AutoSupport. Per eseguire questa funzione è necessario l'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 di avviso.	Mittente trap SNMP

Destinazione	Protocollo	Porta	Descrizione
SNMPv1 o SNMPv3	162/UDP	Utilizzato per inviare trap SNMP di notifica di avviso.	Server fornitore di dati esterno
TCP	2003	Utilizzato per inviare dati sulle prestazioni a un fornitore di dati esterno, come Graphite.	server NTP
NTP	123/UDP	Utilizzato per sincronizzare l'ora sul server Unified Manager con un server orario NTP esterno. (Solo sistemi VMware)	Registro di sistema

Completa il foglio di lavoro

Prima di installare e configurare Unified Manager, è necessario avere a portata di mano informazioni specifiche sul proprio ambiente. 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 distribuito il software	Il tuo valore
Ospita un nome di dominio completamente qualificato	
Indirizzo IP dell'host	
Maschera di rete	
Indirizzo IP del gateway	
Indirizzo DNS primario	
Indirizzo DNS secondario	
Cerca domini	
Nome utente di manutenzione	
Password utente di manutenzione	

Informazioni sulla configurazione di Unified Manager

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

Collocamento	Il tuo valore
Indirizzo email dell'utente addetto alla manutenzione	
Nome host o indirizzo IP del server SMTP	
Nome utente SMTP	
password SMTP	
porta SMTP	25 (valore predefinito)
Email 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 di binding LDAP	
Password di Active Directory o password di binding LDAP	
Nome distinto di base del server di autenticazione	
URL del provider di identità (IdP)	
Metadati del provider di identità (IdP)	
Indirizzi IP dell'host di destinazione della trappola SNMP	
porta SNMP	

Informazioni sul cluster

I dettagli sui sistemi di archiviazione gestiti tramite Unified Manager.

Cluster 1 di N	Il tuo valore
Nome host o indirizzo IP di gestione del cluster	

Cluster 1 di N	Il tuo valore
Nome utente dell'amministratore ONTAP i All'amministratore deve essere stato assegnato il ruolo "admin".	
Password amministratore ONTAP	
Protocollo	HTTPS

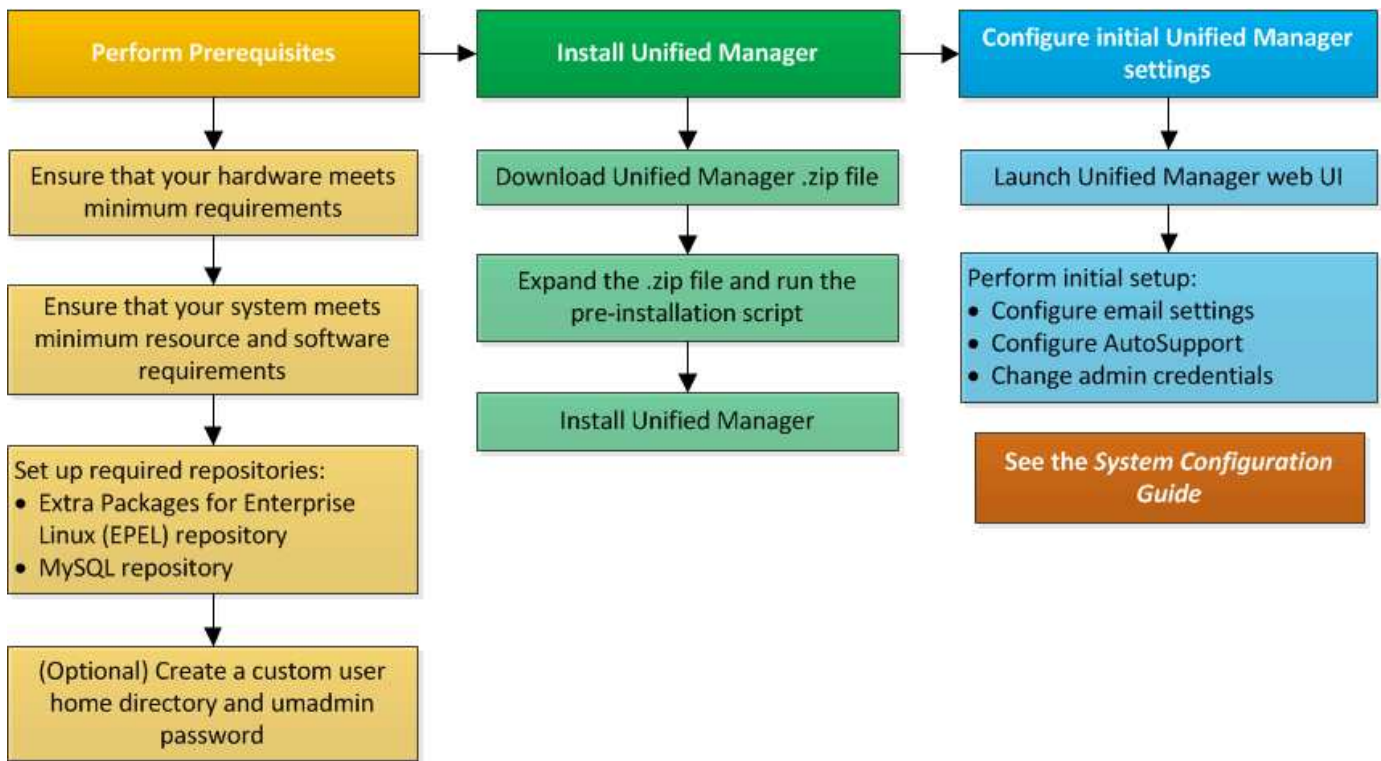
Installa, aggiorna e rimuovi il software Unified Manager

Nei sistemi Linux è possibile installare il software Unified Manager, aggiornarlo a una versione più recente o rimuoverlo.

Unified Manager può essere installato sui server Red Hat Enterprise Linux. Il server Linux su cui si installa Unified Manager può essere in esecuzione 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 che è necessario eseguire prima di poter utilizzare Unified Manager.



Impostare i repository software richiesti

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

Configurare manualmente il repository EPEL

Se il sistema su cui si sta installando Unified Manager non ha accesso al repository Extra Packages for Enterprise Linux (EPEL), è necessario scaricare e configurare manualmente il repository per un'installazione corretta.

Il repository EPEL fornisce l'accesso alle utilità di terze parti necessarie che devono essere installate sul sistema. Per installare Unified Manager su un sistema Red Hat Enterprise Linux, utilizzare il repository EPEL.

Passi

1. Scarica il repository EPEL per la tua installazione. Per la versione 8, scaricala da:

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

Per la versione 9, scaricala da:

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

Configurare manualmente il repository MySQL

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

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



Questa operazione potrebbe non riuscire se il sistema non dispone di connettività Internet. Se il sistema su cui si sta installando Unified Manager non dispone di accesso a Internet, fare riferimento alla documentazione MySQL.

Passi

1. Scarica il repository MySQL appropriato per la tua installazione. Per la versione 8, scaricala da:

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

Per la versione 9, scaricala da:

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

2. Configurare il repository MySQL:

```
yum install mysql84-community-release-.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 disabilitare il repository AppStream e installare MySQL Community Server. Esegui il seguente comando:

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

Se ricevi un errore di chiave mancante o di mancata corrispondenza delle chiavi e l'installazione non riesce, prova questi passaggi:

- 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-2023
```

- Su un sistema che non ha connettività Internet, aggiorna il file del repository MySQL e disabilita gpgcheck marcando gpgcheck=0 .

Requisiti SELinux sulle condivisioni NFS e CIFS

Se stai pianificando di montare `/opt/netapp` o `/opt/netapp/data` su un dispositivo NAS o SAN e hai abilitato SELinux, devi tenere presente alcune considerazioni.

Se stai pianificando di montare `/opt/netapp` o `/opt/netapp/data` da qualsiasi punto diverso dal file system root e se SELinux è abilitato nel tuo ambiente, dovresti impostare il contesto corretto per le directory montate. Per lo scenario applicabile al tuo ambiente, segui questi passaggi per impostare e confermare il contesto SELinux corretto.

Configurare il contesto SELinux quando `/opt/netapp/data` è montato

Se hai montato `/opt/netapp/data` nel tuo 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 del database.

1. Eseguire questo comando per verificare il contesto:

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

Un esempio di output:

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



In questo output, il contesto è `default_t`. Dovresti cambiare questo contesto in `mysqld_db_t`.

2. Eseguire questi passaggi 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 hai configurato `/opt/netapp/data` in `/etc/fstab`, dovresti modificare il `/etc/fstab` file. Per il `/opt/netapp/data/` opzione di montaggio, 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 montaggio 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 se il contesto è impostato correttamente:

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

Un esempio di output:

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

Configurare il contesto SELinux quando `/opt/netapp` è montato, e `/opt/netapp/data/` è montato anche separatamente

In questo scenario, per prima cosa, dovresti 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 padre `/opt/netapp` non ha il contesto SELinux impostato su `file_t`.

Passi

1. Eseguire questo comando per verificare il contesto:

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

Un esempio di output:

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

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

2. Eseguire questi passaggi per impostare il contesto, in base a come 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 hai configurato `/opt/netapp` in `/etc/fstab`, dovresti modificare il `/etc/fstab` file. Per il `/opt/netapp` opzione di montaggio, aggiungere l'etichetta MySQL come:

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

2. Smonta e poi rimonta `/opt/netapp` per abilitare il contesto.
3. Se si dispone di un montaggio 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 se il contesto è impostato correttamente:

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

Un output di esempio

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

Configurare il contesto SELinux quando `/opt/netapp` è montato, e `/opt/netapp/data/` non è montato separatamente

Se hai montato `/opt/netapp` nel tuo 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 del database.

Passi

1. Eseguire questo comando per verificare il contesto:

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

Un esempio di output:

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



In questo output, il contesto è `default_t`. Dovresti cambiare questo contesto in `mysqld_db_t`.

2. Eseguire i seguenti passaggi per impostare il contesto in base al modo in cui è stato montato `/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 hai configurato `/opt/netapp` in `/etc/fstab`, modifica il `/etc/fstab` file. Per il `/opt/netapp/` opzione di montaggio, aggiungere l'etichetta MySQL come:

```
context=system_u:object_r:mysqld_db_t:s0
```
 - c. Smonta e poi rimonta `/opt/netapp/` per abilitare il contesto.
 - d. Se si dispone di un montaggio 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 se il contesto è impostato correttamente:

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

Un esempio di output:

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

Installa Unified Manager sui sistemi Linux

È importante comprendere che la sequenza dei passaggi per scaricare e installare Unified Manager varia a seconda dello scenario di installazione.

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

È possibile creare una directory home 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.

Prima di iniziare

- Il sistema deve soddisfare i requisiti descritti in ["Requisiti di sistema hardware"](#).
- È necessario poter accedere come utente root al sistema Red Hat Enterprise Linux.

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

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

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

Se l'ambiente di installazione richiede di ignorare queste impostazioni di installazione predefinite, seguire questi passaggi per creare una directory home personalizzata e 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 anziché le impostazioni predefinite di installazione.

Inoltre, l'installazione predefinita di Unified Manager include l'utente umadmin nei file sudoers(`ocum_sudoers` e `ocie_sudoers`) nel `/etc/sudoers.d/` elenco. Se rimuovi questo contenuto dal tuo ambiente a causa di policy di sicurezza o di qualche strumento di monitoraggio della sicurezza, devi aggiungerlo di nuovo. È necessario conservare la configurazione sudoers perché alcune operazioni di Unified Manager richiedono questi privilegi sudo.

Le policy di sicurezza del tuo ambiente non devono limitare i privilegi sudo per l'utente addetto alla manutenzione di Unified Manager. Alcune operazioni di Unified Manager potrebbero non riuscire se i privilegi sono limitati. Dopo aver completato correttamente l'installazione, verifica di poter eseguire il seguente comando sudo dopo aver effettuato l'accesso come utente umadmin.

```
sudo systemctl status ocie
```

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

Passi

1. Accedi al server come utente root.
2. Crea l'account del gruppo umadmin denominato “maintenance”:

```
groupadd maintenance
```

3. Crea l'account utente “umadmin” nel gruppo di manutenzione in una directory home a tua scelta:

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

4. Definisci la password umadmin:

```
passwd umadmin
```

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

Dopo aver installato Unified Manager è necessario specificare la shell di accesso dell'utente umadmin.

Scarica Unified Manager

Devi scaricare Unified Manager .zip file dal sito di supporto NetApp per installare Unified Manager.

Prima di iniziare

È necessario disporre delle credenziali di accesso al sito di supporto NetApp .

Scarica il pacchetto di installazione di Unified Manager per il sistema Red Hat Enterprise Linux.

Passi

1. Accedi al sito di supporto NetApp e vai alla pagina di download per 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. Scarica il file di installazione di Unified Manager per Linux e salvalo .zip file in una directory sul sistema di destinazione.



- Assicurati di scaricare la versione corretta del file di installazione per il tuo sistema Red Hat Enterprise Linux. A seconda che tu abbia installato Red Hat Enterprise Linux 8 o 9, assicurati 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 al .zip file.

4. Verificare il checksum per l'integrità del software scaricato.
5. Se hai scaricato il certificato di firma del codice e la firma digitale, puoi 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 del 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 usare.

Installa Unified Manager

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

Prima di iniziare

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

Vedere ["Requisiti di sistema hardware"](#) .

Vedere ["Requisiti di installazione e software Linux"](#) .

- Devi aver scaricato Unified Manager .zip file dal sito di supporto NetApp al sistema di destinazione.
- Avresti dovuto verificare l'integrità del file scaricato .zip file.
- È necessario disporre di un browser web supportato.
- Il software di emulazione del terminale deve avere lo scrollbar abilitato.

Il sistema Red Hat Enterprise Linux potrebbe avere installate tutte le versioni richieste del software di supporto richiesto (Java, MySQL, utilità aggiuntive), solo una parte del software richiesto oppure potrebbe essere un sistema appena installato senza nessuno dei software richiesti.

Passi

1. Accedi al server su cui stai 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 11.0.25	<code>java -version</code>
MySQL 8.4.4 Community Edition	<code>`rpm -qa</code>
<code>grep -i mysql`</code>	<code>p7zip 16.02</code>
<code>`rpm -qa</code>	<code>grep p7zip`</code>

3. Se la versione installata di MySQL è precedente a MySQL 8.4.4 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. Passare alla directory in cui è stato scaricato il file di installazione .zip file 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 dei 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 disabilitare il repository AppStream e installare MySQL Community Server. Esegui il seguente comando:

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

7. **Facoltativo:** è necessario eseguire il passaggio 7 solo se il sistema non è connesso a Internet e se è necessario scaricare manualmente i pacchetti necessari per l'installazione. Se il tuo sistema ha accesso a Internet e tutti i pacchetti richiesti sono disponibili, vai al passaggio 8. Per i sistemi che non sono connessi a Internet o che non utilizzano i repository di Red Hat Enterprise Linux, eseguire i seguenti passaggi per determinare se mancano pacchetti necessari, quindi scaricare tali pacchetti:

- a. Sul sistema su cui stai installando Unified Manager, visualizza l'elenco dei pacchetti disponibili e non disponibili:

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

Gli elementi nella sezione "Installazione:" sono i pacchetti disponibili nella directory corrente, mentre gli elementi nella sezione "Installazione per dipendenze:" sono i pacchetti mancanti nel sistema.

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

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



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. Copia i pacchetti mancanti dal sistema connesso a Internet al tuo 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, tutto l'altro software di supporto necessario e il software Unified Manager.

Se l'installazione fallisce con l'errore GPG NOKEY, utilizzare `rpm --import` per importare le chiavi da un URL:

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



Non tentare l'installazione utilizzando comandi alternativi (ad esempio `rpm -ivh`). Per un'installazione corretta di Unified Manager su un sistema Red Hat Enterprise Linux è necessario che tutti i file di Unified Manager e i file correlati vengano 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 subito dopo i messaggi di installazione.

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

10. Una volta completati i messaggi di installazione, scorrere indietro tra 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 di 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 hai creato un account utente umadmin con una directory home personalizzata prima di installare Unified Manager, devi 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 si installa Unified Manager su Red Hat Enterprise Linux, Unified Manager e utility di terze parti creano i seguenti utenti: umadmin, jboss e mysql.

- **amministratore**

Utilizzato per accedere a Unified Manager per la prima volta. A questo utente è assegnato il ruolo di "Amministratore applicazione" ed è configurato come tipo "Utente manutenzione". Questo utente è stato creato da Unified Manager.

- **jboss**

Utilizzato per eseguire i servizi Unified Manager correlati all'utilità JBoss. Questo utente è stato creato da Unified Manager.

- **mysql**

Utilizzato per eseguire query sul database MySQL di Unified Manager. Questo utente è creato dall'utilità di terze parti MySQL.

Oltre a questi utenti, Unified Manager crea anche i gruppi corrispondenti: manutenzione, jboss e mysql. I gruppi maintenance e jboss vengono creati da Unified Manager, mentre il gruppo mysql viene creato da un'utilità di terze parti.



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

Cambia la password di 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 come utente root al sistema Red Hat Enterprise Linux su cui è installato Unified Manager.
- Devi essere in grado di accedere a NetApp fornito `password.sh` script nella directory `/opt/netapp/essentials/bin`.

Passi

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

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

Non arrestare 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, immettere la nuova password JBoss, quindi inserirla una seconda volta per conferma.

Tieni presente che la password deve essere compresa tra 8 e 16 caratteri e deve contenere almeno una cifra, una lettera maiuscola e una minuscola e almeno uno di questi caratteri speciali:

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

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

```
systemctl start ocie
```

```
systemctl start ocieau
```

6. Dopo aver avviato tutti i servizi, è possibile accedere all'interfaccia utente di Unified Manager.

Aggiorna Unified Manager su Red Hat Enterprise Linux

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

Le patch release del software Unified Manager, quando 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 disconnettere i due prodotti e quindi configurare una nuova connessione Workflow Automation dopo aver eseguito gli aggiornamenti. Se si esegue l'aggiornamento solo a uno dei prodotti, è necessario accedere a Workflow Automation dopo l'aggiornamento 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 ogni versione.

Non tutte le versioni di Unified Manager possono eseguire un aggiornamento sul posto alle versioni successive. Gli aggiornamenti di Unified Manager sono limitati al modello N-2, il che significa che un aggiornamento può essere eseguito solo entro le prossime 2 release su tutte le piattaforme. Ad esempio, è possibile eseguire un aggiornamento a Unified Manager 9.16 solo da Unified Manager 9.13 e 9.14.

Se si utilizza una versione precedente a quelle supportate, sarà necessario prima aggiornare l'istanza di Unified Manager a una delle versioni supportate e poi alla versione corrente.

Ad esempio, se la versione installata è Unified Manager 9.9 e si desidera eseguire l'aggiornamento a Unified Manager 9.14, è necessario seguire una sequenza di aggiornamenti.

Esempio di percorso di aggiornamento:

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

Per ulteriori informazioni sulla matrice del percorso di aggiornamento, vedere questo ["articolo della knowledge base \(KB\)"](#).

Aggiorna Unified Manager

È possibile effettuare l'aggiornamento da Unified Manager 9.13 o 9.14 alla versione 9.16 scaricando ed eseguendo il file di installazione sulla piattaforma Linux.

Prima di iniziare

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

Vedere ["Requisiti di sistema hardware"](#) .

Vedere ["Requisiti di installazione e software Linux"](#) .

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

Vedere ["Aggiornamento di JRE su Linux"](#) .

- Per evitare la perdita di dati, è necessario creare un backup del database di Unified Manager nel caso in cui si verifichi un problema durante l'aggiornamento. NetApp consiglia di spostare il file di backup dal `/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 modificarle in 6 mesi. Dopo la conferma, i dati storici sulle prestazioni vengono eliminati dopo 6 mesi.
- Dovresti aver completato tutte le operazioni in esecuzione, perché 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 di MySQL installata sul sistema è precedente alla 8.4.4, il processo di aggiornamento di Unified Manager aggiorna automaticamente MySQL alla versione 8.4.4.

Passi

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

Vedere ["Scarica Unified Manager per Linux"](#) .

3. Passare 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 dei problemi, è necessario risolverli e procedere con l'aggiornamento.

Se vengono rilevati pacchetti mancanti, eseguire i passaggi indicati in "[Ulteriori passaggi da eseguire per i pacchetti mancanti](#)". Se non mancano pacchetti, procedere con i passaggi successivi.

6. Aggiorna 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 in esecuzione su di essi. 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 dei problemi, è necessario risolverli prima di aggiornare Unified Manager. Se in precedenza sono stati installati pacchetti, ad esempio *net-snmp*, prima di aggiornare Unified Manager, la dipendenza MySQL potrebbe disinstallare il pacchetto durante l'aggiornamento. Per continuare a utilizzarlo, è necessario installare nuovamente il pacchetto manualmente.

7. Una volta completato l'aggiornamento, scorrere i messaggi fino a visualizzare quello che mostra un indirizzo IP o un URL per l'interfaccia utente Web di Unified Manager, il nome utente di 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/
```

Immettere 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 effettuare l'accesso 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 vengono rilevati pacchetti mancanti nel tuo sito, se il tuo sistema non è connesso a Internet o se non stai utilizzando i repository di Red Hat Enterprise Linux, esegui i seguenti passaggi per determinare se mancano pacchetti necessari e scaricarli.



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

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

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

Gli elementi nella sezione "Installazione:" sono i pacchetti disponibili nella directory corrente, mentre gli elementi nella sezione "Installazione per dipendenze:" sono i pacchetti mancanti nel sistema.

2. Su un sistema diverso dotato di accesso a Internet, eseguire il seguente comando per scaricare i pacchetti

mancanti.

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

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

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. Passare alla directory indicata ed eseguire il seguente comando per installare i pacchetti mancanti, insieme alle relative dipendenze.

```
yum install *.rpm
```

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

```
systemctl start ocie
```

```
systemctl start ocieau
```

Questo processo completa il processo di aggiornamento di Unified Manager. Immettere 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 effettuare l'accesso utilizzando lo stesso nome utente di manutenzione (umadmin) e la stessa password impostati in precedenza.

Aggiornare il sistema operativo host da Red Hat Enterprise Linux 7.x a 8.x

Se in precedenza hai installato Unified Manager su un sistema Red Hat Enterprise Linux 7.x e devi eseguire l'aggiornamento a Red Hat Enterprise Linux 8.x, devi 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 e quindi ripristinare il backup su un sistema Red Hat Enterprise Linux 8.x. Si noti che le versioni supportate di Red Hat Enterprise Linux vanno dalla 8.0 alla 8.10.

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, mentre nell'altro caso 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 consigliabile creare il backup solo quando si è pronti a completare l'intero processo di aggiornamento, in modo che Unified Manager resti offline per il minor tempo possibile. Le lacune nei dati raccolti vengono visualizzate nell'interfaccia utente di Unified Manager per il periodo di tempo in cui il sistema Red Hat Enterprise Linux 7.x è spento e prima dell'avvio del nuovo Red Hat Enterprise Linux 8.x.

Vedere ["Gestione delle operazioni di backup e ripristino"](#) se hai bisogno di rivedere le istruzioni dettagliate per i processi di backup e ripristino.

Seguire questi passaggi 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 tale sistema mentre il

sistema Red Hat Enterprise Linux 7.x è ancora disponibile.

1. Installa e configura un nuovo server con il software Red Hat Enterprise Linux 8.x.

Vedere ["Requisiti di installazione e software Linux"](#) .

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

Vedere ["Installazione di Unified Manager su Linux"](#) .

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

3. Nel sistema Red Hat Enterprise Linux 7.x, dal menu Amministrazione nell'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 del repository del database al /database-dumps-repo sottodirectory sotto il /ocum-backup elenco.
6. Immettere il seguente comando per ripristinare il database Unified Manager dal file di backup:

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

7. Inserisci l'indirizzo IP o l'URL nel tuo browser web per avviare l'interfaccia utente web di Unified Manager, quindi accedi al sistema.

Dopo aver 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 di riserva su cui installare il software Red Hat Enterprise Linux 8.x, seguire questi passaggi.

1. Dal menu Amministrazione nell'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.
2. Rimuovere l'immagine di Red Hat Enterprise Linux 7.x dal sistema e cancellare completamente il sistema.
3. Installare e configurare il software Red Hat Enterprise Linux 8.x sullo stesso sistema.

Vedere ["Requisiti di installazione e software Linux"](#) .

4. Sul sistema Red Hat Enterprise Linux 8.x, installa 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 una volta completata l'installazione. Il file di backup inserisce queste informazioni durante il processo di ripristino.

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

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

7. Inserisci l'indirizzo IP o l'URL nel tuo browser web per avviare l'interfaccia utente web di Unified Manager, quindi accedi al sistema.

Aggiornare i 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 vulnerabilità di sicurezza. Puoi effettuare l'aggiornamento alle versioni più recenti di questo software secondo i tuoi tempi.

Aggiorna 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 di sicurezza.

Prima di iniziare

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

È possibile aggiornare le versioni di OpenJDK all'interno delle famiglie di versioni. 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.

Passi

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 Unified Manager:

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

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

```
systemctl start ocie
```

```
systemctl start ocieau
```

Riavvia Unified Manager

Potrebbe essere necessario riavviare Unified Manager dopo aver apportato modifiche

alla configurazione.

Prima di iniziare

È necessario disporre dell'accesso come utente root al server Red Hat Enterprise Linux su cui è installato Unified Manager.

Passi

1. Accedere come utente root al server su cui si desidera riavviare il servizio Unified Manager.
2. Arrestare il servizio Unified Manager e il servizio MySQL associato in questo ordine:

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

```
systemctl stop mysqld
```

3. Avviare i servizi MySQL e Unified Manager in questo ordine:

```
systemctl start mysqld
```

```
systemctl start ocie
```

```
systemctl start ocieau
```



`mysqld` è un programma demone necessario per avviare e arrestare il server MySQL.

Rimuovi Unified Manager

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

Prima di iniziare

- È necessario disporre dell'accesso come utente root al server da cui si desidera rimuovere Unified Manager.
- Security-Enhanced Linux (SELinux) deve essere disabilitato sul sistema Linux. Cambiare la modalità di runtime SELinux in "Permissive" utilizzando `setenforce 0` comando.
- Prima di rimuovere il software, è necessario rimuovere tutti i cluster (origini dati) dal server Unified Manager.
- Dovresti eliminare manualmente le regole del firewall create per consentire o bloccare la porta MySQL 3306. Le regole del firewall non vengono eliminate automaticamente.

Passi

1. Accedi come utente root al server da cui desideri rimuovere Unified Manager.
2. Arrestare e rimuovere Unified Manager dal server:

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

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

3. **Facoltativo:** se appropriato, 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
```

Una volta completata questa operazione, il software verrà rimosso. Tutti i dati dal `/opt/netapp/data` la directory viene spostata in `/opt/netapp/data/BACKUP` cartella dopo la disinstallazione. La disinstallazione di Unified Manager rimuove anche i pacchetti Java e MySQL, a meno che non siano richiesti e utilizzati da altre applicazioni sul sistema. Tuttavia, i dati MySQL non vengono eliminati.

Rimuovere l'utente umadmin personalizzato e il gruppo di manutenzione

Se hai creato una directory home personalizzata per definire il tuo account utente umadmin e di manutenzione prima di installare Unified Manager, dovresti rimuovere questi elementi dopo aver disinstallato Unified Manager.

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

Passi

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

```
userdel umadmin
```

3. Elimina il gruppo di manutenzione:

```
groupdel maintenance
```

Installa Unified Manager sui sistemi Windows

Introduzione ad Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) consente di monitorare e gestire lo stato e le prestazioni dei sistemi di archiviazione ONTAP da un'unica interfaccia. È possibile distribuire Unified Manager su un server Linux, su un server Windows o come appliance virtuale su un host VMware.

Dopo aver completato l'installazione e aver aggiunto i cluster che si desidera gestire, Unified Manager fornisce un'interfaccia grafica che visualizza la capacità, la disponibilità, la protezione e lo stato delle prestazioni dei sistemi di storage monitorati.

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Cosa fa il server Unified Manager

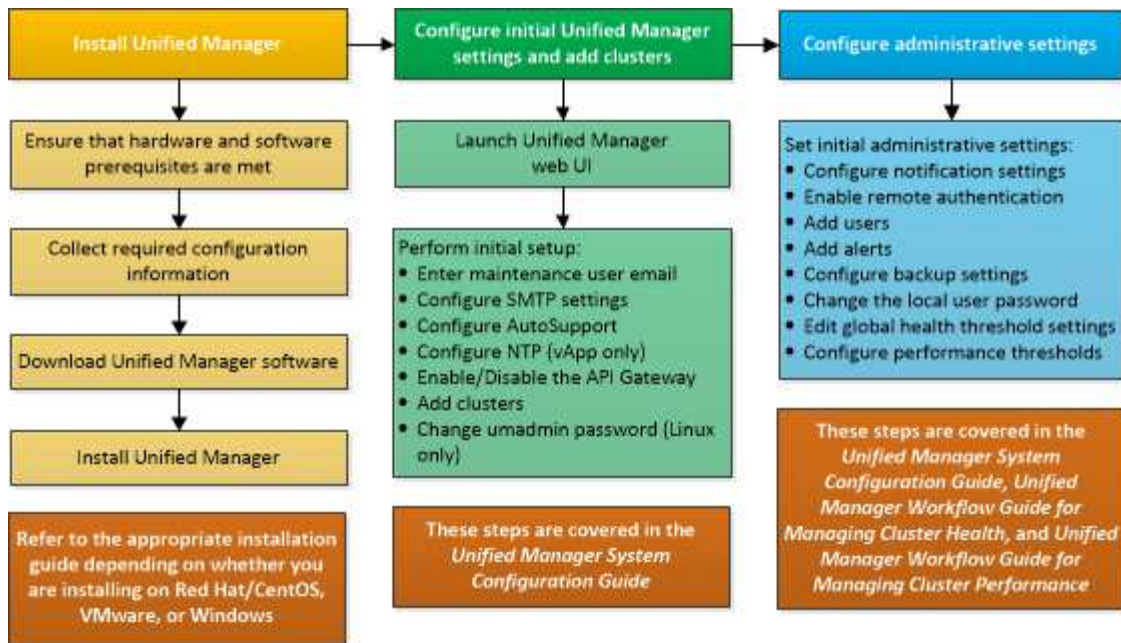
L'infrastruttura del server Unified Manager è composta da un'unità di raccolta dati, un database e un server applicativo. Fornisce servizi infrastrutturali quali individuazione, monitoraggio, controllo degli accessi basato sui ruoli (RBAC), auditing e registrazione.

Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare se ci sono problemi nel cluster.

Panoramica della sequenza di installazione

Il flusso di lavoro di installazione descrive le attività che è necessario eseguire prima di poter utilizzare Unified Manager.

In queste sezioni vengono descritti ciascuno degli elementi mostrati nel flusso di lavoro riportato di seguito.



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 maggiori dettagli sull'applicazione delle misure di sicurezza al server Unified Manager, consultare l'articolo della Knowledge Base.

["Supporto per misure di sicurezza applicate ad Active IQ Unified Manager per Clustered Data ONTAP"](#)

Informazioni correlate

["Strumento matrice di interoperabilità NetApp"](#)

Requisiti di sistema hardware e infrastruttura virtuale

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.

Nella tabella seguente sono riportati 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 prestazioni accettabili.

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

Configurazione hardware	Impostazioni consigliate
Capacità del ciclo della CPU	9572 MHz totali (requisito minimo 9572 MHz)
Spazio libero su disco	150 GB, dove la capacità è 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 memoria sufficiente per prestazioni ottimali e che il sistema possa ospitare cluster e oggetti di archiviazione aggiuntivi man mano che la configurazione cresce. Non dovresti impostare limiti di memoria sulla VM in cui è distribuito Unified Manager e non dovresti abilitare funzionalità (ad esempio, il ballooning) che impediscono al software di utilizzare la memoria allocata sul 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, consultare la *Guida alle best practice*.

["Rapporto tecnico 4621: Guida alle best practice di Unified Manager"](#)

Lo scambio di pagine di memoria ha un impatto negativo sulle prestazioni del sistema e dell'applicazione di gestione. La competizione per risorse della CPU non disponibili a causa dell'utilizzo complessivo dell'host può compromettere le prestazioni.

Requisito per uso 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 prestazioni di Unified Manager.

Requisiti di spazio per i backup

Se si prevede di utilizzare la funzionalità di backup e ripristino di Unified Manager, allocare capacità aggiuntiva in modo che la directory o il disco "data" disponga di 150 GB di spazio. Un backup può essere scritto su una destinazione locale o su una destinazione remota. La procedura consigliata è quella di identificare una posizione remota esterna al sistema host di Unified Manager che disponga di 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 tale da poterlo utilizzare correttamente `ping` il nome host dall'host stesso. In caso di configurazione IPv6, è necessario verificare che `ping6` al nome host ha esito positivo per garantire la corretta installazione di Unified Manager.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web del prodotto. Se hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, hai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, dovresti ottenere il nome host dal DNS.

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

Requisiti di installazione e software Windows

Per installare correttamente Unified Manager su Windows, è necessario assicurarsi che il sistema su cui si desidera installare Unified Manager soddisfi i requisiti software.

Software del sistema operativo

È possibile installare Unified Manager sulle seguenti edizioni di Windows:

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

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

- Inglese
- giapponese
- cinese semplificato

Per l'elenco completo e più aggiornato delle versioni di Windows supportate, consultare la matrice di interoperabilità.

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



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

Il server dovrebbe essere dedicato all'esecuzione di Unified Manager. Non devono essere installate altre applicazioni sul server. È possibile che sul tuo sistema Windows sia installato un software antivirus attivo a causa delle normative aziendali. Per evitare che l'installazione fallisca, è consigliabile disattivare il software antivirus prima di installare Unified Manager.

Software di terze parti

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

- Pacchetti ridistribuibili Microsoft Visual C++ per Visual Studio 2015 versione 14.26.28720.3
- MySQL Community Edition versione 8.4.4
- Python 3.12.4
- OpenJDK versione 11.0.25
- Versione 7-zip 23.01 o successiva



A partire da Unified Manager 9.5, OpenJDK è 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, assicurati che:

- Sta utilizzando la porta predefinita.

- I database di esempio non sono installati.
- Il nome del servizio è "MYSQL84".

Unified Manager è distribuito su un server web WildFly. WildFly 26.1.3 è fornito in bundle e configurato con Unified Manager.



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

Requisiti di installazione

- Deve essere installato 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 sull'interfaccia della riga di comando: `echo %temp%`
- È necessario riservare 2 GB di spazio su disco nell'unità Windows per memorizzare nella cache i file MSI di Unified Manager.
- Il server Microsoft Windows su cui si desidera installare Unified Manager deve essere configurato con un nome di dominio completo (FQDN) in modo tale che ping le risposte al nome host e al nome di dominio completo hanno esito positivo.
- Dovresti disattivare il servizio di pubblicazione Web mondiale di Microsoft IIS e assicurarti che le porte 80 e 443 siano libere.
- Durante l'installazione, assicurarsi che l'impostazione Host sessione Desktop remoto per "Compatibilità RDS di Windows Installer" sia disabilitata.
- La porta UDP 514 deve essere libera e non deve essere utilizzata da nessun altro servizio.
- Prima di installare Unified Manager, dovresti disattivare tutti i software antivirus presenti sul tuo sistema. Una volta completata l'installazione, assicurati di escludere manualmente i seguenti percorsi dalla scansione antivirus:
 - Directory dati Unified Manager, ad esempio, `C:\ProgramData\NetApp\OnCommandAppData\`
 - Directory di installazione di Unified Manager, ad esempio, `\C:\Program Files\NetApp\`
 - Directory 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 dei browser supportate.

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

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

Se si prevede di 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 dall'IdP.

Requisiti di protocollo e porta

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

Connessioni al server Unified Manager

Nelle installazioni tipiche non è necessario specificare i numeri di porta quando ci si connette all'interfaccia utente Web di Unified Manager, perché vengono sempre utilizzate le porte predefinite. Ad esempio, poiché Unified Manager tenta sempre di essere eseguito sulla sua 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
Interfaccia utente web di Unified Manager	HTTP	80	Utilizzato per accedere all'interfaccia utente Web di Unified Manager; reindirizza automaticamente alla porta protetta 443.
Interfaccia utente Web di Unified Manager e 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 tramite HTTPS.
Console di manutenzione	SSH/SFTP	22	Utilizzato per accedere alla console di manutenzione e recuperare i pacchetti di supporto.
Riga di comando di Linux	SSH/SFTP	22	Utilizzato per accedere alla riga di comando di Red Hat Enterprise Linux e recuperare i bundle di supporto.
Registro di sistema	UDP	514	Utilizzato per accedere ai messaggi EMS basati su abbonamento dai sistemi ONTAP e per creare eventi basati sui messaggi.

Interfaccia	Protocollo	Porta	Descrizione
RIPOSO	HTTPS	9443	Utilizzato per accedere in tempo reale agli eventi EMS basati su REST API dai sistemi ONTAP autenticati.
database MySQL	MySQL	3306	Utilizzato per abilitare l'accesso di OnCommand Workflow Automation e OnCommand API Services a Unified Manager.
Broker AMQP QPID	TCP/IP	56072	Utilizzato per la comunicazione di messaggi interni.
Broker AMQP QPID	WebSocket su TCP	56080	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud).
Broker AMQP QPID	WebSocket su TCP	56443	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud). La comunicazione su questa porta supporta la crittografia fornita da TLS o SSL.



La porta predefinita per MySQL, 3306, è limitata solo a localhost durante l'installazione di Unified Manager sui sistemi Windows. Una volta completata l'installazione, abilitare il firewall per limitare l'accesso alla porta MySQL 3306. Ciò non ha alcun impatto sugli scenari 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` opzione sulla console di manutenzione. Per informazioni, vedere ["Opzioni di menu aggiuntive"](#). Le porte utilizzate per la comunicazione HTTP e HTTPS (porte 80 e 443) possono essere modificate tramite la console di manutenzione di Unified Manager. Per maggiori informazioni, vedere ["Configurazione di Active IQ Unified Manager"](#).

Connessioni dal server Unified Manager

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

A seconda dell'ambiente, 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 tramite i seguenti protocolli e porte ai sistemi di archiviazione gestiti, ai server e ad altri componenti:

Destinazione	Protocollo	Porta	Descrizione
Sistema di archiviazione	HTTPS	443/TCP	Utilizzato per monitorare e gestire i sistemi di archiviazione.
Sistema di archiviazione	NDMP	10000/TCP	Utilizzato per determinate operazioni di ripristino Snapshot.
Server AutoSupport	HTTPS	443	Utilizzato per inviare informazioni AutoSupport . Per eseguire questa funzione è necessario l'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 di avviso.	Mittente trap SNMP
SNMPv1 o SNMPv3	162/UDP	Utilizzato per inviare trap SNMP di notifica di avviso.	Server fornitore di dati esterno
TCP	2003	Utilizzato per inviare dati sulle prestazioni a un fornitore di dati esterno, come Graphite.	server NTP
NTP	123/UDP	Utilizzato per sincronizzare l'ora sul server Unified Manager con un server orario NTP esterno. (Solo sistemi VMware)	Broker AMQP QPID

Destinazione	Protocollo	Porta	Descrizione
TCP/IP	56072	Utilizzato per la comunicazione di messaggi interni.	Broker AMQP QPID
WebSocket su TCP	56080	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud).	Broker AMQP QPID
WebSocket su TCP	56443	Utilizzato per ascoltare su questa porta i messaggi ricevuti da ONTAP (agente cloud). La comunicazione tramite questa porta supporta la crittografia fornita da TLS o SSL.	Registro di sistema

Completa il foglio di lavoro

Prima di installare e configurare Unified Manager, è necessario avere a portata di mano informazioni specifiche sul proprio ambiente. 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 distribuito il software	Il tuo valore
Ospita un nome di dominio completamente qualificato	
Indirizzo IP dell'host	
Maschera di rete	
Indirizzo IP del gateway	
Indirizzo DNS primario	
Indirizzo DNS secondario	
Cerca domini	
Nome utente di manutenzione	

Sistema su cui viene distribuito il software	Il tuo valore
Password utente di manutenzione	

Informazioni sulla configurazione di Unified Manager

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

Collocamento	Il tuo valore
Indirizzo email dell'utente addetto alla manutenzione	
Nome host o indirizzo IP del server SMTP	
Nome utente SMTP	
password SMTP	
porta SMTP	25 (valore predefinito)
Email 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 di binding LDAP	
Password di Active Directory o password di binding LDAP	
Nome distinto di base del server di autenticazione	
URL del provider di identità (IdP)	
Metadati del provider di identità (IdP)	
Indirizzi IP dell'host di destinazione della trappola SNMP	
porta SNMP	

Informazioni sul cluster

I dettagli sui sistemi di archiviazione gestiti tramite Unified Manager.

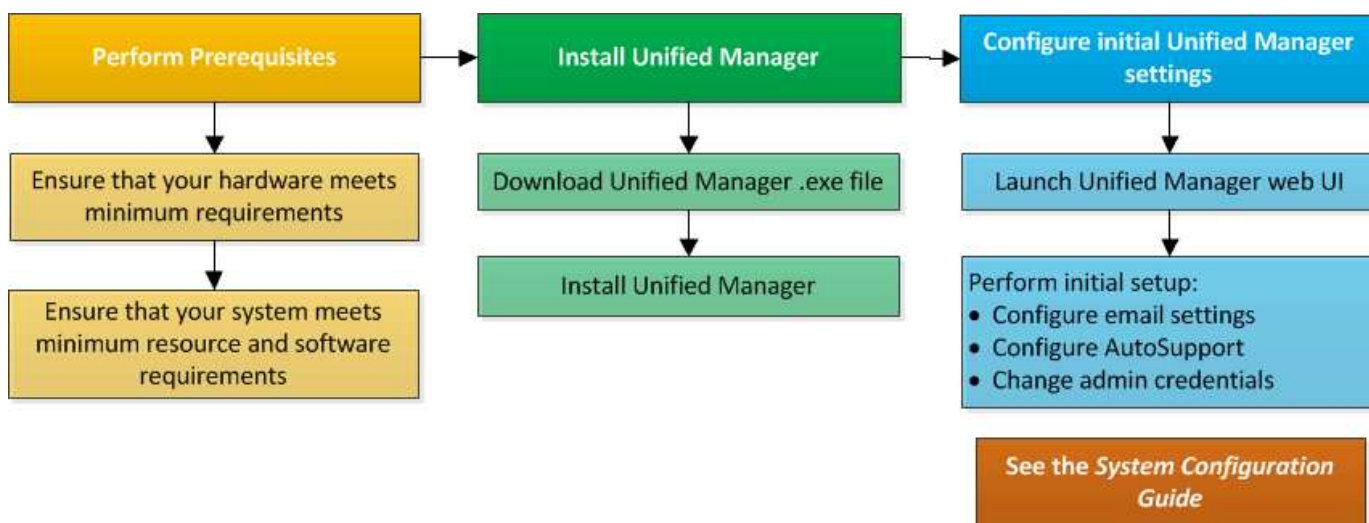
Cluster 1 di N	Il tuo valore
Nome host o indirizzo IP di gestione del cluster	
Nome utente dell'amministratore ONTAP i All'amministratore deve essere stato assegnato il ruolo "admin".	
Password amministratore ONTAP	
Protocollo	HTTPS

Installa, aggiorna e rimuovi il 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 che è necessario eseguire prima di poter utilizzare Unified Manager.



Installa Unified Manager su Windows

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

Installa Unified Manager

È possibile installare Unified Manager per monitorare e risolvere i problemi relativi a capacità di archiviazione dei dati, disponibilità, prestazioni e protezione.

Prima di iniziare

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

Vedere ["Requisiti di sistema hardware"](#) .

Vedere ["Requisiti di installazione e software Windows"](#) .



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

- Dovresti avere privilegi di amministratore di Windows. Assicurati che il tuo 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 "!".
- Sono supportati tutti i cluster, ad eccezione dei sistemi ASA r2.
- Dovresti avere un browser web supportato.
- La password utente di manutenzione di Unified Manager deve essere compresa tra 8 e 20 caratteri e contenere lettere maiuscole o minuscole, numeri e caratteri speciali.
- I seguenti caratteri speciali non sono consentiti nella stringa della password per l'utente addetto alla manutenzione o per l'utente root di MySQL: " ' ` % , = & < > | ^ \ / () [] ; :

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

Passi

1. Accedi a Windows utilizzando l'account amministratore locale predefinito.
2. Accedi al sito di supporto NetApp e vai alla pagina di download per 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 per Windows o il file zip in una directory di destinazione sul sistema Windows.
5. Se necessario, estrarre il file zip e andare alla directory in cui si trova il file di installazione.
6. Fare clic con il pulsante destro del mouse ed eseguire il file eseguibile (.exe) del programma di installazione di Unified Manager 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. Inserisci il nome utente e la password per creare l'utente addetto alla manutenzione.
9. Nella procedura guidata di connessione al database, immettere la password di root di MySQL.
10. Fare clic su **Modifica** 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 verrà installato nella directory di installazione predefinita.

11. Fare clic su **Avanti**.
12. Nella procedura guidata Ready to Install Shield, fare clic su **Installa**.
13. Una volta completata l'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 dati di Unified Manager
 - Directory di installazione di Unified Manager
 - Directory dei dati MySQL

L'installazione crea più directory:

- Directory di installazione

Questa è la directory radice di Unified Manager, specificata durante l'installazione. Esempio: C:\Program Files\NetApp\

- Directory dei dati MySQL

Questa è la directory in cui sono archiviati i database MySQL, specificati 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 Unified Manager (appDataDir)

Questa è la directory in cui vengono archiviati tutti i dati generati dall'applicazione. Ciò include registri, pacchetti 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](#)".

Eseguire 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.

Passi

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

Opzione	Istruzioni
Se sono preinstallati pacchetti di terze parti	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qn /l*v CompletePathForLogFile"</pre> Esempio: <pre>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"</pre>
Se non sono installati pacchetti di terze parti	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qr /l*v CompletePathForLogFile"</pre> Esempio: <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MySQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</pre>

IL /qr l'opzione abilita la modalità silenziosa con un'interfaccia utente ridotta. Viene visualizzata un'interfaccia utente di base che mostra l'avanzamento dell'installazione. Non ti verrà richiesto di immettere dati. Se i pacchetti di terze parti come JRE, MySQL e 7zip non sono preinstallati, dovresti usare /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 abilita la modalità silenziosa senza interfaccia utente. Durante l'installazione non vengono visualizzati né l'interfaccia utente né i dettagli. Non dovresti usare il /qn opzione quando non sono installati pacchetti di terze parti.

3. Accedi all'interfaccia utente web di Unified Manager utilizzando il seguente URL:

`https://IP address`

Cambia la password di 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.

Prima di iniziare

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

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

Passi

1. Accedi 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 NetApp Active IQ Management Server (Oncommandsvc)
3. Avviare il `password.bat` script per iniziare il processo di modifica della password:

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

4. Quando richiesto, immettere la password dell'utente root di MySQL.
5. Quando richiesto, immettere la nuova password utente JBoss, quindi inserirla nuovamente per conferma.

Tieni presente che la password deve essere compresa tra 8 e 16 caratteri e deve contenere almeno una cifra, una lettera maiuscola e una minuscola e almeno uno di questi caratteri speciali:

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

6. Al termine dello script, avviare i servizi Unified Manager utilizzando la console Servizi Windows:
 - Servizio NetApp Active IQ Management Server (Oncommandsvc)
 - Servizio di acquisizione NetApp Active IQ (Ocie-au)
7. Dopo aver avviato 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 ogni versione.

Non tutte le versioni di Unified Manager possono eseguire un aggiornamento sul posto alle versioni successive. Gli aggiornamenti di Unified Manager sono limitati al modello N-2, il che significa che un aggiornamento può essere eseguito solo entro le prossime 2 release su tutte le piattaforme. Ad esempio, è possibile eseguire un aggiornamento a Unified Manager 9.16 solo da Unified Manager 9.13 e 9.14.

Se si utilizza una versione precedente a quelle supportate, sarà necessario prima aggiornare l'istanza di Unified Manager a una delle versioni supportate e poi alla versione corrente.

Ad esempio, se la versione installata è Unified Manager 9.9 e si desidera eseguire l'aggiornamento a Unified Manager 9.14, è necessario seguire una sequenza di aggiornamenti.

Esempio di percorso di aggiornamento:

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

Per ulteriori informazioni sulla matrice del percorso di aggiornamento, vedere questo ["articolo della knowledge base \(KB\)"](#).

Aggiorna Unified Manager

È possibile aggiornare Unified Manager 9.13 o 9.14 alla versione 9.16 scaricando ed eseguendo il file di installazione sulla piattaforma Windows.

Prima di iniziare

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

Vedere ["Requisiti di sistema hardware"](#).

Vedere ["Requisiti di installazione e software Windows"](#).



A partire da Unified Manager 9.5, OpenJDK è 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 di MySQL installata sul sistema è precedente alla 8.4.4, il processo di aggiornamento di Unified Manager aggiorna automaticamente MySQL alla versione 8.4.4. Non è consentito eseguire un aggiornamento autonomo di una versione precedente di MySQL alla versione 8.4.4.
- Sono supportati tutti i cluster, ad eccezione dei sistemi ASA r2.
- Dovresti avere privilegi di amministratore di Windows. Assicurati che il tuo 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 sito di supporto NetApp è necessario disporre di credenziali valide.
- Per evitare la perdita di dati, è opportuno creare un backup della macchina Unified Manager nel caso in cui

si verifichi un problema durante l'aggiornamento.

- Per eseguire l'aggiornamento è necessario disporre di spazio su disco sufficiente.

Lo spazio disponibile sull'unità di installazione deve essere 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 non c'è abbastanza spazio libero.

- Durante l'aggiornamento, potrebbe esserti richiesto di confermare se desideri mantenere le impostazioni predefinite precedenti per la conservazione dei dati sulle prestazioni per 13 mesi o modificarle in 6 mesi. Dopo la conferma, i dati storici sulle prestazioni dopo 6 mesi vengono eliminati.
- Prima di eseguire l'aggiornamento, chiudere tutti i file o le cartelle aperti in *<InstallDir>\JDK e MySQL Data Directory*.
- Se sul sistema Windows è installato un software antivirus attivo, l'aggiornamento di Unified Manager potrebbe non riuscire. Prima di aggiornare Unified Manager, dovresti disattivare tutti i software antivirus presenti sul tuo sistema.

Durante il processo di aggiornamento, Unified Manager non è disponibile. Prima di aggiornare 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 disconnettere i due prodotti e quindi configurare una nuova connessione Workflow Automation dopo aver eseguito gli aggiornamenti. Se si esegue l'aggiornamento solo a uno dei prodotti, è necessario accedere a Workflow Automation dopo l'aggiornamento e verificare che stia ancora acquisendo dati da Unified Manager.

Passi

1. Accedi al sito di supporto NetApp e vai alla pagina di download per 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 Windows o il file zip in una directory di destinazione sul sistema Windows. Se necessario, estrarre il file zip e andare alla directory in cui si trova il file di installazione. Fare clic con il pulsante destro del mouse ed eseguire il file eseguibile (.exe) del programma di installazione di Unified Manager come amministratore.

Unified Manager visualizza il seguente messaggio:

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

4. Fare clic su **Sì**, quindi su **Avanti**.
5. Immettere la password di root di MySQL84 impostata durante l'installazione, quindi fare clic su **Avanti**.
6. Avvia l'interfaccia utente Web in una nuova finestra su un browser Web supportato ed effettua l'accesso per utilizzare la versione aggiornata di Unified Manager.
7. 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 dati di Unified Manager

- Directory di installazione di Unified Manager
- Directory dei dati MySQL



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

Aggiornare i prodotti di terze parti

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

Le aziende che sviluppano questi prodotti di terze parti segnalano regolarmente vulnerabilità di sicurezza. Puoi effettuare l'aggiornamento alle versioni più recenti di questo software secondo i tuoi tempi.

Aggiorna 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 di sicurezza.

Prima di iniziare

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

È possibile aggiornare le versioni di OpenJDK all'interno delle famiglie di versioni. Ad esempio, è possibile eseguire l'aggiornamento da OpenJDK 11.0.16 a OpenJDK 11.0.18, ma non è possibile eseguire l'aggiornamento direttamente da OpenJDK 11 a OpenJDK 12.

Passi

1. Accedi 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 `jdk-11.0.18_windows-x64_bin.zip` from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html>.



Per scaricare il file è necessario un account Oracle. Se non hai un account Oracle, vai a "[Accesso all'account Oracle](#)" pagina per crearne una.

3. Utilizzare la console dei servizi Windows per arrestare i seguenti servizi di Unified Manager:
 - Servizio di acquisizione NetApp Active IQ (Ocie-au)
 - Servizio NetApp Active IQ Management Server (Oncommandsvc)
4. Espandi il zip file.
5. Copiare le directory e i file dal file risultante jdk directory (ad esempio, `jdk-11.0.18` alla posizione in cui è installato Java. Esempio: `C:\Program Files\NetApp\JDK\`
6. Avviare i servizi Unified Manager utilizzando la console Servizi Windows:
 - Servizio NetApp Active IQ Management Server (Oncommandsvc)

- Servizio di acquisizione NetApp Active IQ (Ocie-au)

Disinstallare i prodotti di terze parti

Dopo aver aggiornato Unified Manager, puoi disinstallare prodotti di terze parti, come Python o Microsoft Visual C++ 2013. Questo è facoltativo.

Disinstallare Python

Passi

1. Dal **Pannello di controllo** seleziona **Programmi > Programmi e funzionalità**.
2. Selezionare Python dall'elenco dei programmi.
3. Seleziona **Disinstalla questo programma**. Disinstallare qualsiasi versione di Python tranne la 3.12. Assicurati di mantenere la versione 3.12 di Python.

Disinstallare Microsoft Visual C++ 2013

Passi

1. Dal **Pannello di controllo** seleziona **Programmi > Programmi e funzionalità**.
2. Selezionare **Microsoft Visual C++ 2013** dall'elenco dei programmi.
3. Seleziona **Disinstalla questo programma**.

Riavvia Unified Manager

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

Prima di iniziare

È necessario disporre dei privilegi di amministratore di Windows.

Passi

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

Dal...	Arrestare i servizi nel seguente ordine...
Riga di comando	a. <code>sc stop ocie-au</code> b. <code>sc stop Oncommandsvc</code>
Microsoft Service Manager	a. Servizio di acquisizione NetApp Active IQ (Ocie-au) b. Servizio NetApp Active IQ Management Server (Oncommandsvc)

3. Avviare i servizi Unified Manager:

Dal...	Avviare i servizi nel seguente ordine...
Riga di comando	a. <code>sc start Oncommandsvc</code> b. <code>sc start ocie-au</code>
Microsoft Service Manager	a. Servizio NetApp Active IQ Management Server (Oncommandsvc) b. Servizio di acquisizione NetApp Active IQ (Ocie-au)

Disinstallare Unified Manager

È possibile disinstallare Unified Manager utilizzando la procedura guidata Programmi e funzionalità oppure eseguendo una disinstallazione automatica dall'interfaccia della riga di comando.

Prima di iniziare

- È necessario disporre dei privilegi di amministratore di Windows.
- Prima di disinstallare il software, è necessario rimuovere tutti i cluster (origini dati) dal server Unified Manager.
- Dovresti eliminare manualmente le regole del firewall create per consentire o bloccare la porta MySQL 3306. Le regole del firewall non vengono eliminate automaticamente.

Passi

1. Disinstallare Unified Manager scegliendo una delle seguenti opzioni:

- Se si disinstalla Unified Manager tramite la procedura guidata **Programmi e funzionalità**, procedere come segue:
 - i. Vai su **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, procedere come segue:
 - i. Accedi alla riga di comando di Windows utilizzando i privilegi di amministratore.
 - ii. Passare 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 sul server è abilitato il Controllo account utente (UAC) e si è effettuato l'accesso come utente di dominio, è necessario utilizzare il metodo di disinstallazione dalla riga di comando.

Unified Manager è stato 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++ 2015 Redistributable, Python e 7zip

- Dati dell'applicazione MySQL generati da Unified Manager
- Registri delle applicazioni e contenuto della directory dei dati delle applicazioni

Eseguire attività di configurazione e amministrative

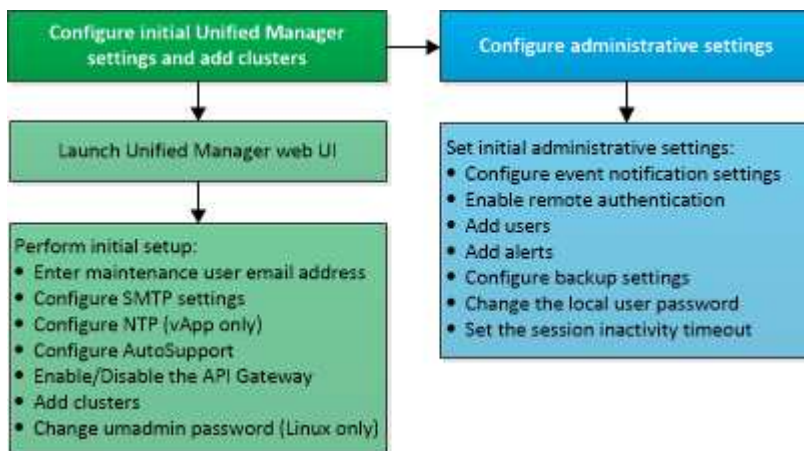
Configura Active IQ Unified Manager

Dopo aver installato Active IQ Unified Manager (in precedenza OnCommand Unified Manager), 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, come 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 impostazioni di configurazione consigliate che è utile impostare sulla nuova istanza o che è bene conoscere prima di iniziare il monitoraggio regolare dei sistemi ONTAP.

Panoramica della sequenza di configurazione

Il flusso di lavoro di configurazione descrive le attività che è necessario eseguire prima di poter utilizzare Unified Manager.



Accedi all'interfaccia utente web di Unified Manager

Dopo aver installato Unified Manager, puoi accedere all'interfaccia utente Web per configurare Unified Manager e iniziare a monitorare i tuoi sistemi ONTAP.

Prima di iniziare

- Se è la prima volta che accedi all'interfaccia utente Web, devi effettuare l'accesso come utente di manutenzione (o utente umadmin per le installazioni Linux).
- Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve anziché 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 accettare il rischio di continuare l'accesso oppure installare un certificato digitale firmato da un'autorità di certificazione (CA) per l'autenticazione del server.

Passi

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 il nome di dominio completo (FQDN) del server Unified Manager.

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

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



Se effettui tre tentativi consecutivi di accesso all'interfaccia utente web senza successo nell'arco di un'ora, verrai bloccato fuori dal sistema e dovrai contattare l'amministratore di sistema. Questa opzione è valida solo per gli utenti locali.

Eseguire la configurazione iniziale dell'interfaccia utente Web di Unified Manager

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

Prima di iniziare

Devi aver eseguito le seguenti operazioni:

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

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

☰

Active IQ Unified Manager

All ▾

Search All Storage Objects and Actions 🔍

Getting Started

1

2

3

4

5

EmailAutoSupportAPI GatewayAdd ONTAP ClustersFinish

Notifications

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

Maintenance User Email

Email

mgo@eng.netapp.com

SMTP Server

Host Name or IP Address

email.eng.netapp.com

Port

25

User Name

admin

Password

☐ Use STARTTLS ⓘ☐ Use SSL ⓘ

Continue

Se in seguito desideri modificare una di queste opzioni, puoi selezionarla dalle opzioni Generali nel riquadro di navigazione a sinistra di Unified Manager. Si noti che l'impostazione NTP è valida solo per le installazioni VMware e può essere modificata in seguito tramite la console di manutenzione di Unified Manager.

Passi

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



Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver cliccato sul pulsante **Continua** verrà visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per continuare con le impostazioni di configurazione iniziale dell'interfaccia utente Web.

2. Nella pagina AutoSupport fare clic su **Accetta 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 , oppure se si desidera disattivare AutoSupport, utilizzare l'opzione **Generale** > * AutoSupport*

dall'interfaccia utente Web.

3. Nei sistemi Red Hat, modificare la password dell'utente umadmin dalla stringa predefinita "admin" a una stringa personalizzata.
4. Nella pagina Configura API Gateway, seleziona se desideri utilizzare la funzionalità API Gateway che consente a Unified Manager di gestire i cluster ONTAP che intendi monitorare tramite le API REST ONTAP. Quindi fare clic su **Continua**.

È possibile abilitare o disabilitare questa impostazione in un secondo momento nell'interfaccia utente Web da **Generale > Impostazioni funzionalità > API Gateway**. Per ulteriori informazioni sulle API, vedere ["Introduzione alle API REST Active IQ Unified Manager"](#).

5. Aggiungere i cluster che si desidera vengano gestiti da Unified Manager, quindi fare clic su **Avanti**. Per ogni cluster che intendi gestire, devi disporre del nome host o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6) insieme alle credenziali di nome utente e 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 **Gestione archiviazione > Configurazione cluster**.

6. Nella pagina Riepilogo, verifica che tutte le impostazioni siano corrette e fai clic su **Fine**.

La pagina Introduzione si chiude e viene visualizzata la pagina Dashboard di Unified Manager.

Aggiungi cluster

È possibile aggiungere un cluster ad Active IQ Unified Manager in modo da poterlo monitorare. Ciò include la possibilità di ottenere informazioni sul cluster, quali integrità, capacità, prestazioni e configurazione del cluster, in modo da poter individuare e risolvere eventuali problemi che potrebbero verificarsi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario disporre delle seguenti informazioni:
 - Unified Manager supporta cluster ONTAP on-premise, ONTAP Select Cloud Volumes ONTAP.
 - Nome host o indirizzo IP di gestione del cluster

Il nome host è il nome FQDN o 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 il LIF di gestione del cluster della macchina virtuale di archiviazione amministrativa (SVM). Se si utilizza un LIF di gestione dei nodi, l'operazione fallisce.

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

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

- Il numero di porta per connettersi al cluster tramite il protocollo HTTPS (in genere la porta 443)
- Hai i certificati richiesti:

Certificato SSL (HTTPS): Questo certificato è di proprietà di Unified Manager. Con una nuova installazione di Unified Manager viene generato un certificato SSL autofirmato predefinito (HTTPS). NetApp consiglia di aggiornarlo al certificato firmato da una 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 sicurezza HTTPS"](#) .

Certificato EMS: Questo certificato è di proprietà di Unified Manager. Viene utilizzato durante l'autenticazione per le notifiche EMS ricevute da ONTAP.

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 ONTAP . Se il cluster che esegue la versione ONTAP è precedente alla 9.5, l'autenticazione basata su certificato non è abilitata.

L'autenticazione basata su certificato non viene abilitata automaticamente per un cluster se si aggiorna una versione precedente di Unified Manager. Tuttavia, è possibile abilitarlo 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"](#) .



- È possibile aggiungere un cluster dall'interfaccia utente Web e l'autenticazione basata su certificato verrà abilitata automaticamente.
- È possibile aggiungere un cluster tramite Unified Manager CLI; l'autenticazione basata su certificato non è abilitata per impostazione predefinita. Se si aggiunge un cluster tramite Unified Manager CLI, è necessario modificare il cluster tramite l'interfaccia utente di Unified Manager. Puoi vedere ["Comandi CLI di Unified Manager supportati"](#) per aggiungere un cluster utilizzando Unified Manager CLI.
- Se per un cluster è abilitata l'autenticazione basata su certificato e si esegue il backup di Unified Manager da un server e lo si ripristina su un altro server Unified Manager in cui il nome host o l'indirizzo IP è stato modificato, il monitoraggio del cluster potrebbe non riuscire. Per evitare il fallimento, modificare e salvare i dettagli del cluster. Per ulteriori informazioni sulla modifica dei dettagli del cluster, vedere ["Modifica dei cluster"](#) .

+

Certificati cluster: Questo certificato è di proprietà di ONTAP. Non è possibile aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato è già scaduto, è necessario rigenerarlo prima di aggiungere il cluster. Per informazioni sulla generazione del certificato, consultare l'articolo della knowledge base (KB) ["Come rinnovare un certificato autofirmato ONTAP nell'interfaccia utente di System Manager"](#) .

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

Per una configurazione MetroCluster , è necessario aggiungere sia il cluster locale che quello remoto e i cluster devono essere configurati correttamente.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.
2. Nella pagina Configurazione cluster, fare clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi cluster, specificare i valori richiesti, come 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 ciclo di monitoraggio successivo.

4. Fare clic su **Invia**.
5. Nella finestra di dialogo Autorizza host, fare clic su **Visualizza certificato** per visualizzare le informazioni sul certificato del cluster.
6. Fare clic su **Sì**.

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.

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



Poiché la raccolta di 15 giorni di dati sulle prestazioni richiede un uso intensivo della CPU, si consiglia di scaglionare l'aggiunta di nuovi cluster in modo che i sondaggi sulla 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 verrà interrotta e si vedranno delle lacune nei grafici delle prestazioni per il periodo di tempo mancante.



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

Informazioni correlate

["Installazione di un certificato HTTPS firmato e restituito da una CA"](#)

Configurare Unified Manager per inviare notifiche di avviso

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Dopo aver distribuito Unified Manager e completato la configurazione iniziale, dovresti prendere in considerazione la possibilità di configurare l'ambiente in modo da attivare avvisi e generare e-mail di notifica o trap SNMP in base alla ricezione di eventi.

Passi

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

Se si desidera che vengano inviate notifiche di avviso quando si verificano determinati eventi nel proprio ambiente, è necessario configurare un server SMTP e fornire un indirizzo e-mail da cui verrà inviata la notifica di avviso. Se si desidera utilizzare trap SNMP, è possibile selezionare tale opzione e fornire le informazioni necessarie.

2. "Abilita 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 abilitare l'autenticazione remota.

3. "Aggiungi 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. "Aggiungi utenti".

È possibile aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando si crea un avviso, si assegna un utente che riceverà le notifiche di avviso.

5. "Aggiungi avvisi".

Dopo aver aggiunto l'indirizzo email per l'invio delle notifiche, aggiunto gli utenti che riceveranno le notifiche, configurato le impostazioni di rete e configurato le opzioni SMTP e SNMP necessarie per il tuo ambiente, puoi assegnare gli avvisi.

Configurare le impostazioni di notifica degli eventi

È possibile configurare Unified Manager in modo che invii notifiche di avviso quando viene generato un evento o quando un evento viene assegnato 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.

Prima di iniziare

È necessario disporre delle seguenti informazioni:

- Indirizzo email da cui viene inviata la notifica di avviso

L'indirizzo email appare nel campo "Da" nelle notifiche di avviso inviate. Se per qualsiasi motivo l'e-mail non può essere recapitata, questo indirizzo e-mail viene utilizzato anche come destinatario per la posta non recapitata.

- Nome host del server SMTP e nome utente e password per accedere al server
- Nome host o indirizzo IP per l'host di destinazione della trappola che riceverà la trappola SNMP, insieme alla versione SNMP, alla porta della trappola in uscita, alla community e ad altri valori di configurazione SNMP richiesti

Per specificare più destinazioni trap, separare ogni host con una virgola. In questo caso, tutte le altre impostazioni SNMP, come la versione e la porta trap in uscita, devono essere le stesse per tutti gli host

nell'elenco.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

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

Note:

- Se l'indirizzo del mittente è precompilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", dovresti modificarlo con un indirizzo email reale e funzionante per assicurarti che tutte le notifiche email vengano recapitate correttamente.
- Se non è possibile risolvere il nome host del server SMTP, è possibile specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP anziché il nome host.

3. Fare clic su **Salva**.
4. Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver fatto clic sul pulsante **Salva** verrà visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per salvare le impostazioni di notifica.

È possibile fare clic sul pulsante **Visualizza dettagli certificato** per visualizzare i dettagli del certificato. Se il certificato esistente è scaduto, deseleziona la casella **Usa STARTTLS** o **Usa SSL**, salva le impostazioni di notifica e seleziona nuovamente la casella **Usa STARTTLS** o **Usa SSL** per visualizzare un nuovo certificato.

Abilita l'autenticazione remota

È possibile abilitare 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 gli oggetti di archiviazione e i dati.

Prima di iniziare

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, ad esempio SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

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

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



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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Seleziona la casella **Abilita autenticazione remota....**
3. Nel campo Servizio di autenticazione, seleziona il tipo di servizio e configura il servizio di autenticazione.

Per il tipo di autenticazione...	Inserisci le seguenti informazioni...
Directory attiva	• 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)
Apri LDAP	• Associa nome distinto (nella notazione LDAP appropriata) • Password di collegamento • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o scade, è probabile che il server di autenticazione stia impiegando molto tempo a 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 tramite il protocollo Secure Sockets Layer (SSL).

4. **Facoltativo:** Aggiungi server di autenticazione e testa l'autenticazione.
5. Fare clic su **Salva**.

Disabilita i gruppi nidificati dall'autenticazione remota

Se è abilitata l'autenticazione remota, è possibile disabilitare l'autenticazione di gruppo nidificata in modo che solo i singoli utenti, e non i membri del gruppo, possano autenticarsi in remoto su Unified Manager. È possibile disabilitare i gruppi nidificati quando si desidera migliorare il tempo di risposta dell'autenticazione di Active Directory.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione.
- La disabilitazione 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 per i gruppi nidificati è disabilitato e se un gruppo remoto viene aggiunto a Unified Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Seleziona la casella **Disabilita ricerca gruppi annidati**.
3. Fare clic su **Salva**.

Impostare i servizi di autenticazione

I servizi di autenticazione consentono l'autenticazione di utenti 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) oppure configurando un proprio meccanismo di autenticazione.

Prima di iniziare

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Seleziona uno dei seguenti servizi di autenticazione:

Se selezioni...	Allora fai così...
Directory attiva	a. Inserisci 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 <code>ou@domain.com</code>, il nome distinto di base è cn=ou,dc=domain,dc=com.
OpenLDAP	a. Immettere il nome distinto e la password di associazione. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è <code>ou@domain.com</code>, il nome distinto di base è cn=ou,dc=domain,dc=com.

Se selezioni...	Allora fai così...
Altri	a. Immettere il nome distinto e la password di associazione. 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 utente e gli attributi del membro.



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

3. Fare clic su **Salva**.

Aggiungi 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.

Prima di iniziare

- 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 abilitato 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) (che utilizza 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Abilita o disabilita l'opzione **Usa connessione sicura**:

Se lo desidera...	Allora fai così...
Abilitarlo	a. Selezionare l'opzione Usa connessione protetta. b. Nell'area Server di autenticazione, fare clic su Aggiungi. c. Nella finestra di dialogo 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 sul certificato, quindi fare clic su Chiudi. f. Nella finestra di dialogo Autorizza host, fare clic su Sì.  Quando si abilita l'opzione Usa autenticazione connessione protetta, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza la porta 636 come porta predefinita per le comunicazioni protette e la porta 389 per le comunicazioni non protette.
Disabilitarlo	a. Deselezionare l'opzione Usa connessione protetta. b. Nell'area Server di autenticazione, fare clic su Aggiungi. c. Nella finestra di dialogo 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.

- Esegui un'autenticazione di prova per confermare che puoi autenticare gli utenti nel server di autenticazione che hai aggiunto.

Testare la 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 cercando un utente o un gruppo remoto dai server di autenticazione e autenticandolo tramite le impostazioni configurate.

Prima di iniziare

- È necessario aver abilitato 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 aver aggiunto i server di autenticazione affinché il server di gestione possa cercare l'utente 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 di utenti remoti che appartengono al gruppo primario del server di autenticazione, le informazioni sul gruppo primario non vengono visualizzate nei risultati dell'autenticazione.

Passi

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

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

Aggiungi avvisi

È possibile configurare degli avvisi per essere avvisati quando viene generato un evento specifico. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un tipo di gravità specifico. È possibile specificare la frequenza con cui si desidera ricevere la notifica e associare uno script all'avviso.

Prima di iniziare

- È necessario aver configurato le impostazioni di notifica, quali l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP, per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento.
- 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 a cui si desidera inviare la notifica.
- Se si desidera che uno script venga eseguito in base all'evento, è necessario aver aggiunto lo script a Unified Manager tramite la pagina Script.
- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Impostazione avviso, come descritto qui.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina Impostazione avvisi, fare clic su **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 **Il nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse che corrispondono alla regola del filtro. La stringa di testo specificata è sensibile alla distinzione tra maiuscole e minuscole.

Se una risorsa è conforme sia alle regole di inclusione che a quelle di 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 gravità dell'evento per cui si desidera attivare un avviso.



Per selezionare più di un evento, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **Azioni** e selezionare gli utenti a cui si desidera inviare la notifica, scegliere la frequenza della 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 email specificato per l'utente e si riapre l'avviso per modificarlo, il campo Nome appare vuoto perché l'indirizzo email modificato non è più associato all'utente precedentemente selezionato. Inoltre, se hai modificato l'indirizzo email dell'utente selezionato dalla pagina Utenti, l'indirizzo email modificato non verrà aggiornato per l'utente selezionato.

È anche possibile scegliere di avvisare gli utenti tramite trap SNMP.

7. Fare clic su **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 essere avvisato ogni 15 minuti

Eseguire i seguenti passaggi nella finestra di dialogo Aggiungi avviso:

Passi

1. Fare clic su **Nome** e immettere **HealthTest** nel campo **Nome avviso**.
2. Fare clic su **Risorse** e, nella scheda Includi, selezionare **Volumi** dall'elenco a discesa.
 - a. Immettere **abc** nel campo **Il nome contiene** per visualizzare i volumi il cui nome contiene "abc".
 - b. Seleziona **+ [All Volumes whose name contains 'abc'] +** dall'area Risorse disponibili e spostarlo nell'area Risorse selezionate.
 - c. Fare clic su **Escludi** e immettere **xyz** nel campo **Il nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **Critico** dal campo Gravità evento.

4. Seleziona **Tutti gli eventi critici** dall'area Eventi corrispondenti e spostalo nell'area Eventi selezionati.
5. Fare clic su **Azioni** e immettere **sample@domain.com** nel campo Avvisa questi utenti.
6. Seleziona **Ricorda ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

È possibile configurare un avviso in modo che invii ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario stabilire l'orario a partire dal quale la notifica dell'evento è attiva per l'avviso.

7. Nel menu Seleziona script da eseguire, seleziona script **Test**.
8. Fare clic su **Salva**.

Cambia la password dell'utente locale

È possibile modificare la password di accesso dell'utente locale per prevenire potenziali rischi per la sicurezza.

Prima di iniziare

Devi aver effettuato l'accesso come utente locale.

Le password per l'utente addetto alla manutenzione e per gli utenti remoti non possono essere modificate seguendo questi passaggi. Per modificare la password di un utente remoto, contattare l'amministratore delle password. Per modificare la password dell'utente addetto alla manutenzione, vedere "[Utilizzo della console di manutenzione](#)".

Passi

1. Accedi a Unified Manager.
2. Dalla barra dei menu in alto, fare clic sull'icona dell'utente e quindi su **Cambia password**.

L'opzione **Cambia password** non viene visualizzata se sei un utente remoto.

3. Nella finestra di dialogo Cambia password, immettere la password corrente e quella nuova.
4. Fare clic su **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.

Imposta il 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 inattività. Per impostazione predefinita, il timeout è impostato su 4.320 minuti (72 ore).

Prima di iniziare

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 abilitata l'autenticazione Security Assertion Markup Language (SAML).

Passi

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

Se lo desidera...	Allora fai così...
Non impostare alcun timeout in modo che la sessione non venga mai chiusa automaticamente	Nel pannello Timeout di inattività , spostare il cursore verso sinistra (off) e fare clic su Applica .
Imposta un numero specifico di minuti come valore di timeout	Nel pannello Timeout di inattività , spostare il cursore verso destra (on), specificare il valore del timeout di inattività in minuti e fare clic su Applica .

Imposta il timeout della sessione tramite CLI

È possibile impostare un valore massimo di timeout della sessione per Unified Manager tramite la CLI, in modo che la sessione venga terminata automaticamente dopo un determinato periodo di tempo. Per impostazione predefinita, il timeout della sessione è impostato sul valore massimo, ovvero 4.320 minuti (72 ore). Ciò significa che la sessione termina automaticamente dopo 72 ore, anche se hai effettuato l'accesso e stai utilizzando attivamente Unified Manager.

Informazioni su questo compito

È necessario disporre del ruolo di amministratore dell'applicazione.

L'impostazione del timeout della sessione ha effetto su tutte le sessioni degli utenti registrati.

Passi

1. Accedi alla CLI di Unified Manager immettendo un `cli login` comando. Utilizzare un nome utente e una password validi per l'autenticazione.
2. Entra nel `um option set max.session.timeout.value=<in mins>` comando per modificare il valore di timeout della sessione.

Cambiare il nome host di Unified Manager

A un certo punto, potresti voler modificare il nome host del sistema su cui hai installato Unified Manager. Ad esempio, potresti voler rinominare l'host per identificare più facilmente i server Unified Manager in base al tipo, al gruppo di lavoro o al gruppo di cluster monitorati.

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

Modificare il nome host dell'appliance virtuale Unified Manager

All'host di rete viene assegnato un nome quando l'appliance virtuale Unified Manager viene distribuita per la prima volta. È possibile modificare il nome host dopo la

distribuzione. Se si modifica il nome host, è necessario rigenerare anche il certificato HTTPS.

Prima di iniziare

Per eseguire queste attività, è necessario aver effettuato l'accesso a Unified Manager come utente addetto alla manutenzione oppure 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 hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, allora avrai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, il nome host dovrebbe 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 sicurezza.

Indipendentemente da come è stato assegnato il 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 sicurezza.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server anziché il 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 nel 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 avrà effetto finché non verrà riavviata la macchina virtuale Unified Manager.

Passi

1. [Genera un certificato di sicurezza 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 Unified Manager](#)

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

Genera un certificato di sicurezza 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 sicurezza HTTPS che sostituisca quello esistente.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

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

Se non si ha 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 di validità della chiave. Se usi il `Reset Server Certificate` opzione dalla console di manutenzione, viene creato un nuovo certificato HTTPS valido per 397 giorni. Questo

certificato avrà una chiave RSA di dimensione 2048 bit.

Passi

1. Nel riquadro di navigazione 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 di come si desidera generare il certificato:

Se lo desidera...	Fai questo...
Rigenera il certificato con i valori correnti	Fare clic sull'opzione Rigenera utilizzando gli attributi del certificato corrente .

Se lo desidera...	Fai questo...
Generare il certificato utilizzando valori diversi	Fare clic sull'opzione Aggiorna gli attributi del certificato corrente. Se non si immettono nuovi valori, i campi Nome comune e Nomi alternativi utilizzeranno i valori del certificato esistente. Il ``Nome comune' dovrebbe essere impostato sul nome di dominio completo (FQDN) dell'host. Gli altri campi non richiedono valori, ma è possibile immettere valori, ad esempio, per EMAIL, AZIENDA, REPARTO, Città, Stato e Paese se si desidera che tali valori vengano compilati nel certificato. È anche possibile selezionare tra le DIMENSIONI DELLA CHIAVE disponibili (l'algoritmo della chiave è "RSA") e il 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. Sebbene sia consentito un periodo di validità di 36.500 giorni, si consiglia di utilizzare un periodo di validità non superiore a 397 giorni o 13 mesi. Poiché se selezioni un periodo di validità superiore a 397 giorni e intendi esportare una CSR per questo certificato e farla firmare da una CA nota, la validità del certificato firmato restituito dalla CA verrà ridotta a 397 giorni. • È possibile selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad esempio localhost)" se si desidera rimuovere le informazioni di identificazione locali dal campo Nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi verrà utilizzato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

4. Fare clic su **Si** per rigenerare il certificato.
5. Riavviare il server Unified Manager affinché il nuovo certificato abbia effetto.
6. Verificare le informazioni del nuovo certificato visualizzando il certificato HTTPS.

Riavviare la macchina virtuale Unified Manager

È possibile riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. È necessario riavviare dopo aver generato un nuovo certificato di sicurezza o se si verifica un problema con la macchina virtuale.

Prima di iniziare

L'appliance virtuale è accesa.

Hai effettuato l'accesso alla console di manutenzione come utente addetto alla manutenzione.

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

Passi

1. Accedere alla console di manutenzione.
2. Selezionare **Configurazione di sistema > Riavvia macchina virtuale**.

Modificare il nome host di Unified Manager sui sistemi Linux

A un certo punto, potresti voler modificare il nome host del computer Red Hat Enterprise Linux su cui hai installato Unified Manager. Ad esempio, potresti voler rinominare l'host per identificare più facilmente i server Unified Manager in base al tipo, al gruppo di lavoro o al gruppo di cluster monitorati quando elenchi i tuoi computer Linux.

Prima di iniziare

È necessario disporre dell'accesso come 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 hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, allora avrai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, il nome host dovrebbe essere preso dal server DNS.

Indipendentemente da come è stato assegnato il 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 sicurezza.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server anziché il 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 nel certificato corrisponda al nome host effettivo. Il nuovo certificato non avrà effetto finché non verrà riavviato il computer 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.

Passi

1. Accedi come utente root al sistema Unified Manager che desideri modificare.

2. Arrestare il software Unified Manager e il software MySQL associato immettendo il seguente comando:

```
systemctl stop ocieau ocie mysqld
```

3. Cambia il nome host usando 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:

```
systemctl restart NetworkManager.service
```

6. Dopo aver riavviato il servizio, verificare se il nuovo nome host è in grado di eseguire il ping su se stesso:

```
ping new_hostname
```

```
ping nuhost
```

Questo comando dovrebbe restituire lo stesso indirizzo IP impostato in precedenza 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
```

Abilitare e disabilitare la gestione dell'archiviazione basata su policy

A partire da Unified Manager 9.7, è possibile eseguire il provisioning di carichi di lavoro di archiviazione (volumi e LUN) sui cluster ONTAP e gestire tali carichi di lavoro in base ai livelli di servizio delle prestazioni assegnati. Questa funzionalità è simile alla creazione di carichi di lavoro in ONTAP System Manager e all'associazione di policy QoS, ma quando applicata tramite Unified Manager è possibile eseguire il provisioning e gestire i carichi di lavoro su tutti i cluster monitorati dall'istanza di Unified Manager.

È necessario disporre del ruolo di amministratore dell'applicazione.

Questa opzione è abilitata per impostazione predefinita, ma è possibile disabilitarla se non si desidera eseguire il provisioning e gestire i carichi di lavoro tramite Unified Manager.

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

Nuovi contenuti	Posizione
Una pagina per il provisioning di nuovi carichi di lavoro	Disponibile da Attività comuni > Provisioning
Una pagina per creare policy di livello di servizio delle prestazioni	Disponibile da Impostazioni > Criteri > Livelli di servizio delle prestazioni
Una pagina per creare policy di efficienza di archiviazione delle prestazioni	Disponibile da Impostazioni > Criteri > Efficienza di archiviazione
Pannelli che descrivono le prestazioni del carico di lavoro e gli IOPS del carico di lavoro attuali	Disponibile dalla Dashboard

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disabilita o abilita la gestione dell'archiviazione basata su criteri scegliendo una delle seguenti opzioni:

Se lo desidera...	Allora fai così...
Disabilitare la gestione dell'archiviazione basata su policy	Nel pannello Gestione dell'archiviazione basata su criteri , spostare il cursore verso sinistra.
Abilita la gestione dell'archiviazione basata su policy	Nel pannello Gestione dell'archiviazione basata su criteri , spostare il cursore verso destra.

Configurare il backup di Unified Manager

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

Per informazioni sui passaggi di configurazione, vedere "[Gestione delle operazioni di backup e ripristino](#)".

Gestisci le impostazioni delle funzionalità

La pagina Impostazioni funzionalità consente di abilitare e disabilitare funzionalità specifiche in Active IQ Unified Manager. Ciò include la creazione e la gestione di oggetti di archiviazione in base a criteri, l'abilitazione di API Gateway e Login Banner, 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 disabilitazione della ricezione di eventi della piattaforma Active IQ.



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

Per informazioni sul caricamento degli script, vedere ["Abilitazione e disabilitazione del caricamento degli script"](#).

Abilita la gestione dell'archiviazione basata su policy

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

Attivando questa funzionalità, è possibile eseguire il provisioning dei carichi di lavoro di archiviazione sui cluster ONTAP aggiunti all'istanza di Active IQ Unified Manager e gestire tali carichi di lavoro in base ai livelli di servizio delle prestazioni assegnati e ai criteri di efficienza dell'archiviazione.

Puoi scegliere di attivare o disattivare questa funzionalità da **Generale > Impostazioni funzionalità > Gestione dell'archiviazione basata su criteri**. Attivando questa funzione, sono disponibili le seguenti pagine per il funzionamento e il monitoraggio:

- Provisioning (provisioning del carico di lavoro di archiviazione)
- **Politiche > Livelli di servizio prestazionali**
- **Politiche > Efficienza di archiviazione**
- Colonna Carichi di lavoro gestiti dal livello di servizio delle prestazioni nella pagina Configurazione cluster
- Pannello Prestazioni del carico di lavoro nella **Dashboard**

È possibile utilizzare le schermate per creare livelli di servizio delle prestazioni e policy di efficienza dell'archiviazione, nonché per eseguire il provisioning dei carichi di lavoro di archiviazione. È inoltre possibile monitorare i carichi di lavoro di archiviazione conformi ai livelli di servizio delle prestazioni assegnati, nonché quelli non conformi. Il pannello Prestazioni del carico di lavoro e IOPS del carico di lavoro consente inoltre di valutare la capacità e le prestazioni (IOPS) totali, disponibili e utilizzate dei cluster nel data center in base ai carichi di lavoro di storage in essi forniti.

Dopo aver attivato questa funzionalità, è possibile eseguire le API REST di Unified Manager per svolgere alcune di queste funzioni dalla categoria **Barra dei menu > Pulsante Guida > Documentazione API > provider di archiviazione**. In alternativa, puoi immettere il nome host o l'indirizzo IP e l'URL per accedere alla pagina REST API nel formato `https://<hostname>/docs/api/`

Per ulteriori informazioni sulle API, vedere ["Introduzione alle API REST Active IQ Unified Manager"](#).

Abilita API Gateway

La funzionalità API Gateway consente ad Active IQ Unified Manager di essere un unico piano di controllo da cui è possibile gestire più cluster ONTAP, senza doverli accedere singolarmente.

È possibile abilitare questa funzionalità dalle pagine di configurazione che vengono visualizzate al primo accesso a Unified Manager. In alternativa, puoi abilitare o disabilitare questa funzione da **Generale > Impostazioni funzione > API Gateway**.

Le API REST di Unified Manager sono diverse dalle API REST ONTAP e non tutte le funzionalità delle API

REST ONTAP possono essere sfruttate utilizzando le API REST di Unified Manager. Tuttavia, se si ha un requisito aziendale specifico di accesso alle API ONTAP per la gestione di funzionalità specifiche non esposte a Unified Manager, è possibile abilitare la funzionalità API Gateway ed eseguire le API ONTAP. Il gateway funge da proxy per incanalare le richieste API mantenendo l'intestazione e il corpo delle richieste 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 dover passare le credenziali individuali del cluster. Unified Manager funge da singolo punto di gestione per l'esecuzione delle API sui 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 abilitato questa funzionalità, è possibile eseguire le API REST di Unified Manager dalla **Barra dei menu > Pulsante Guida > Documentazione API > categoria gateway**. In alternativa, puoi immettere il nome host o l'indirizzo IP e l'URL per accedere alla pagina REST API nel formato <https://<hostname>/docs/api/>

Per ulteriori informazioni sulle API, vedere ["Introduzione alle API REST Active IQ Unified Manager"](#).

Specificare il 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 automaticamente disconnessa. Questa opzione è abilitata per impostazione predefinita.

È possibile disattivare questa funzione o modificare il tempo da **Generale > Impostazioni funzione > Timeout di inattività**. Una volta attivata questa funzione, è necessario specificare il limite di tempo di inattività (in minuti) nel campo **DISCONNETTITI DOPO**, dopo il quale il sistema si disconnetterà automaticamente. Il valore predefinito è 4320 minuti (72 ore).



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

Abilita gli eventi del portale Active IQ

È possibile specificare se abilitare o disabilitare gli eventi del portale Active IQ. Questa impostazione consente al portale Active IQ di scoprire e visualizzare eventi aggiuntivi sulla configurazione del sistema, sul cablaggio e così via. Questa opzione è abilitata per impostazione predefinita.

Abilitando questa funzionalità, Active IQ Unified Manager visualizza gli eventi rilevati dal portale Active IQ. Questi eventi vengono creati eseguendo una serie di regole sui messaggi AutoSupport generati da tutti i sistemi di archiviazione monitorati. Questi eventi sono diversi dagli altri eventi di Unified Manager e identificano incidenti o rischi correlati alla configurazione del sistema, al cablaggio, alle best practice e ai problemi di disponibilità.

Puoi scegliere di attivare o disattivare questa funzione da **Generale > Impostazioni funzione > Eventi Active IQ ***. **Nei siti senza accesso alla rete esterna, è necessario caricare manualmente le regole da *Gestione archiviazione > Impostazione evento > Carica regole**.

Questa funzione è abilitata per impostazione predefinita. La disattivazione di questa funzione impedisce che gli eventi Active IQ vengano rilevati o visualizzati su Unified Manager. Se disabilitata, l'abilitazione di questa funzionalità consente a Unified Manager di ricevere gli eventi Active IQ su un cluster all'ora predefinita 00:15 per quel fuso orario del cluster.

Abilita e disabilita le impostazioni di sicurezza per la conformità

Utilizzando il pulsante **Personalizza** nel pannello **Dashboard di sicurezza** della pagina Impostazioni funzionalità, è possibile abilitare o disabilitare i parametri di sicurezza per il monitoraggio della conformità su Unified Manager.

Le impostazioni abilitate o disabilitate da questa pagina regolano lo stato di conformità generale dei cluster e delle VM di archiviazione su Unified Manager. In base alle selezioni, le colonne corrispondenti sono visibili nella vista **Sicurezza: tutti i cluster** della pagina Inventario cluster e nella vista **Sicurezza: tutte le VM di storage** della pagina Inventario VM di storage.



Solo gli utenti con ruolo di amministratore possono modificare queste impostazioni.

I criteri di sicurezza per i cluster ONTAP, le VM di archiviazione e i volumi vengono valutati in base alle raccomandazioni definite in "[Guida al rafforzamento della sicurezza per NetApp ONTAP 9](#)". Il pannello Sicurezza nella dashboard e la pagina Sicurezza mostrano lo stato di conformità di sicurezza predefinito dei cluster, delle VM di archiviazione e dei volumi. Vengono inoltre generati eventi di sicurezza e abilitate azioni di gestione per i cluster e le VM di storage che presentano violazioni della sicurezza.

Personalizza le impostazioni di sicurezza

Per personalizzare le impostazioni per il monitoraggio della conformità in base al tuo ambiente ONTAP, segui questi passaggi:

Passi

1. Fare clic su **Generale > Impostazioni funzionalità > Dashboard di sicurezza > Personalizza**. Viene visualizzata la finestra pop-up **Personalizza impostazioni dashboard di sicurezza**.



I parametri di conformità alla sicurezza abilitati o disabilitati possono influire direttamente sulle visualizzazioni di sicurezza predefinite, sui report e sui report pianificati nelle schermate Cluster e VM di archiviazione. Se hai caricato un report Excel da queste schermate prima di modificare i parametri di sicurezza, i report Excel scaricati potrebbero essere difettosi.

2. Per abilitare o disabilitare le impostazioni personalizzate per i cluster ONTAP, selezionare l'impostazione generale richiesta in **Cluster**. Per informazioni sulle opzioni per la personalizzazione della conformità del cluster, vedere "[Categorie di conformità del cluster](#)".
3. Per abilitare o disabilitare le impostazioni personalizzate per le VM di archiviazione, selezionare l'impostazione generale richiesta in **VM di archiviazione**. Per informazioni sulle opzioni per la personalizzazione della conformità della VM di archiviazione, vedere "[Categorie di conformità delle VM di archiviazione](#)".

Personalizza le impostazioni di AutoSupport e autenticazione

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 abilitare la generazione di avvisi Unified Manager per l'utente amministratore ONTAP predefinito.

Abilita e disabilita il caricamento degli script

La possibilità di caricare script su Unified Manager ed eseguirli è abilitata per impostazione predefinita. Se la tua organizzazione non desidera consentire questa attività per motivi di sicurezza, puoi disattivare questa funzionalità.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disabilita o abilita gli script scegliendo una delle seguenti opzioni:

Se lo desidera...	Allora fai così...
Disabilita gli script	Nel pannello Caricamento script , spostare il cursore verso sinistra.
Abilita gli script	Nel pannello Caricamento script , spostare il cursore verso destra.

Aggiungi banner di accesso

L'aggiunta di un banner di accesso consente alla tua organizzazione di visualizzare qualsiasi informazione, ad esempio chi è autorizzato ad accedere al sistema e i termini e le condizioni d'uso durante l'accesso e la disconnessione.

Qualsiasi utente, come gli operatori o gli amministratori di storage, può visualizzare questo banner pop-up di accesso durante l'accesso, la disconnessione e il timeout della sessione.

Utilizzare 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 possibili problemi.

Quali funzionalità fornisce la console di manutenzione

La console di manutenzione di Unified Manager consente di gestire 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 installato Unified Manager, la console di manutenzione fornisce le seguenti funzioni:

- Risolvi eventuali problemi con il tuo dispositivo virtuale, soprattutto se l'interfaccia web di Unified Manager non è disponibile

- Aggiorna alle versioni più recenti di Unified Manager
- Genera pacchetti di supporto da inviare al supporto tecnico
- Configurare le impostazioni di rete
- Cambia la password dell'utente addetto alla manutenzione
- Connettiti a un fornitore di dati esterno per inviare statistiche sulle prestazioni
- Modificare la raccolta dati sulle prestazioni interna
- Ripristinare il database e le impostazioni di configurazione di Unified Manager da una versione precedentemente sottoposta a backup.

Cosa fa l'utente addetto alla manutenzione

L'utente addetto alla manutenzione viene creato durante l'installazione di Unified Manager su un sistema Red Hat Enterprise Linux. Il nome utente addetto alla manutenzione è "umadmin". L'utente addetto alla manutenzione ha il ruolo di amministratore dell'applicazione nell'interfaccia utente Web e può creare utenti successivi e assegnare loro ruoli.

L'utente addetto alla manutenzione, o utente umadmin, può anche accedere alla console di manutenzione di Unified Manager.

Capacità diagnostiche dell'utente

Lo scopo dell'accesso diagnostico è consentire al supporto tecnico di assisterti nella risoluzione dei problemi e dovresti utilizzarlo solo quando indicato dal supporto tecnico.

L'utente diagnostico può eseguire comandi a livello di sistema operativo quando richiesto dal supporto tecnico, per scopi di risoluzione dei problemi.

Accedi 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.

Prima di iniziare

È necessario aver installato e configurato Unified Manager.

Dopo 15 minuti di inattività, la console di manutenzione effettua la disconnessione.



Se installato su VMware, se hai già effettuato l'accesso come utente di manutenzione tramite la console VMware, non puoi effettuare l'accesso contemporaneamente tramite Secure Shell.

Fare un passo

1. Per accedere alla console di manutenzione, seguire questi passaggi:

Su questo sistema operativo...	Segui questi passaggi...
VMware	- Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo dell'appliance virtuale Unified Manager. - Accedi alla console di manutenzione utilizzando il tuo nome utente e la tua password di manutenzione.
Linux	- Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager. - Accedi al sistema con il nome utente di manutenzione (umadmin) e la password. - Inserisci il comando <code>maintenance_console</code> e premere Invio.
Finestre	- Accedi al sistema Unified Manager con le credenziali di amministratore. - Avvia PowerShell come amministratore di Windows. - Inserisci il comando <code>maintenance_console</code> e premere Invio.

Viene visualizzato il menu della console di manutenzione di Unified Manager.

Accedi alla console di manutenzione tramite 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.

Prima di iniziare

- Devi essere l'utente addetto alla manutenzione.
- Per accedere alla console di manutenzione, l'appliance virtuale deve essere accesa.

Passi

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 effettuare l'accesso.
4. Accedi alla console di manutenzione utilizzando il tuo nome utente e la tua password.

Dopo 15 minuti di inattività, la console di manutenzione effettua la disconnessione.

Menu della console di manutenzione

La console di manutenzione è composta da diversi menu che consentono di gestire e gestire funzionalità speciali e impostazioni di configurazione del server Unified Manager.

A seconda del sistema operativo su cui è installato Unified Manager, la console di manutenzione è composta dai seguenti menu:

- Aggiorna Unified Manager (solo VMware)
- Configurazione di rete (solo VMware)
- Configurazione del sistema (solo VMware)
 - a. Supporto/Diagnostica
 - b. Reimposta il certificato del server
 - c. Fornitore di dati esterno
 - d. Backup Ripristino
 - e. Configurazione dell'intervallo di polling delle prestazioni
 - f. Disabilitare l'autenticazione SAML
 - g. Visualizza/modifica le porte dell'applicazione
 - h. Configurazione del registro di debug
 - i. Controlla l'accesso alla porta MySQL 3306
 - j. Uscita

Per accedere all'opzione di menu specifica, selezionare il numero dall'elenco. Ad esempio, per il backup e il ripristino, selezionare 4.

Menu di 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 o su Microsoft Windows.

Sono disponibili le seguenti opzioni di menu.

• Visualizza impostazioni indirizzo IP

Visualizza le impostazioni di rete correnti per l'appliance virtuale, tra cui indirizzo IP, rete, indirizzo broadcast, netmask, gateway e server DNS.

• Modifica le impostazioni dell'indirizzo IP

Consente di modificare qualsiasi impostazione di rete per l'appliance virtuale, tra cui l'indirizzo IP, la maschera di rete, il gateway o i server DNS. Se si modificano le impostazioni di rete da DHCP a rete statica tramite la console di manutenzione, non è possibile modificare il nome host. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

• Visualizza impostazioni di ricerca del nome di dominio

Visualizza l'elenco di ricerca dei nomi di dominio utilizzati per risolvere i nomi host.

- **Modifica le impostazioni di ricerca del nome di dominio**

Consente di modificare i nomi di dominio che si desidera cercare durante la risoluzione dei nomi host. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Visualizza percorsi statici**

Visualizza le rotte di rete statiche correnti.

- **Modifica percorsi statici**

Consente di aggiungere o eliminare percorsi di rete statici. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Aggiungi percorso**

Consente di aggiungere una route statica.

- **Elimina percorso**

Consente di eliminare una route statica.

- **Indietro**

Ti riporta al **Menu principale**.

- **Uscita**

Esce dalla console di manutenzione.

- **Disabilita interfaccia di rete**

Disabilita tutte le interfacce di rete disponibili. Se è disponibile una sola interfaccia di rete, non è possibile disattivarla. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Abilita interfaccia di rete**

Abilita le interfacce di rete disponibili. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Applica modifiche**

Applica tutte le modifiche apportate alle impostazioni di rete per l'appliance virtuale. È necessario selezionare questa opzione per rendere effettive le modifiche apportate, altrimenti le modifiche non verranno applicate.

- **Ping un host**

Esegue il ping di un host di destinazione per confermare le modifiche dell'indirizzo IP o le configurazioni DNS.

- **Ripristina le impostazioni predefinite**

Ripristina tutte le impostazioni ai valori predefiniti di fabbrica. Per rendere effettive le modifiche, è

necessario selezionare **Importa modifiche**.

- **Indietro**

Ti riporta al **Menu principale**.

- **Uscita**

Esce dalla console di manutenzione.

Menu di configurazione del sistema

Il menu Configurazione di sistema consente di gestire l'appliance virtuale fornendo varie opzioni, come la visualizzazione dello stato del server e 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 "Ripristina da un backup di Unified Manager".

Sono disponibili le seguenti opzioni di menu:

- **Visualizza lo stato del server**

Visualizza lo stato attuale del server. Le opzioni di stato includono In esecuzione e Non in esecuzione.

Se il server non è in esecuzione, potrebbe essere necessario contattare l'assistenza tecnica.

- **Riavvia la macchina virtuale**

Riavvia la macchina virtuale, arrestando tutti i servizi. Dopo il riavvio, la macchina virtuale e i servizi vengono riavviati.

- **Spegnimento della macchina virtuale**

Arresta la macchina virtuale, interrompendo tutti i servizi.

È possibile selezionare questa opzione solo dalla console della macchina virtuale.

- **Cambia la password dell'utente <utente registrato>**

Modifica la password dell'utente attualmente connesso, che può essere solo l'utente addetto alla manutenzione.

- **Aumenta la dimensione del disco dati**

Aumenta la dimensione del disco dati (disco 3) nella macchina virtuale.

- **Aumenta la dimensione del disco di swap**

Aumenta la dimensione del disco di swap (disco 2) nella macchina virtuale.

- **Cambia fuso orario**

Modifica il fuso orario in base alla tua posizione.

- **Cambia server NTP**

Modifica le impostazioni del server NTP, come l'indirizzo IP o il nome di dominio completo (FQDN).

- **Cambia servizio NTP**

Passa tra `ntp` E `systemd-timesyncd` servizi.

- **Ripristina da un backup di Unified Manager**

Ripristina il database e le impostazioni di configurazione di Unified Manager da una versione precedentemente sottoposta a backup.

- **Reimposta certificato server**

Reimposta il certificato di sicurezza del server.

- **Cambia nome host**

Modifica il nome dell'host su cui è installata l'appliance virtuale.

- **Indietro**

Esce dal menu Configurazione di sistema e torna al menu principale.

- **Uscita**

Esce dal menu della console di manutenzione.

Menu Supporto e Diagnostica

Il menu Supporto e diagnostica consente di generare un pacchetto di supporto da inviare al supporto tecnico per ricevere assistenza nella risoluzione dei problemi.

Sono disponibili le seguenti opzioni di menu:

- **Genera pacchetto di supporto leggero**

Consente di produrre un pacchetto di supporto leggero che contiene solo 30 giorni di registri e record del database di configurazione, escludendo i dati sulle prestazioni, i file di registrazione delle acquisizioni e il dump dell'heap del server.

- **Genera pacchetto di supporto**

Consente di creare un pacchetto di supporto completo (file 7-Zip) contenente informazioni diagnostiche nella directory home dell'utente diagnostico. Se il tuo sistema è connesso a Internet, puoi anche caricare il pacchetto di supporto su NetApp.

Il file include informazioni generate da un messaggio AutoSupport , il contenuto del database Unified Manager, dati dettagliati sugli elementi interni del server Unified Manager e registri dettagliati normalmente non 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:

- **Reimposta certificato server**

Rigenera il certificato del server HTTPS.

È possibile rigenerare il certificato del server nell'interfaccia utente grafica di Unified Manager facendo clic su **Generale > Certificati HTTPS > Rigenera certificato HTTPS**.

- **Disabilita l'autenticazione SAML**

Disabilita 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 in genere utilizzata quando un problema con il server IdP o la configurazione SAML impedisce agli utenti di accedere all'interfaccia utente grafica di Unified Manager.

- **Fornitore di dati esterno**

Fornisce opzioni per connettere Unified Manager a un fornitore di dati esterno. Dopo aver stabilito la connessione, i dati sulle prestazioni vengono inviati a un server esterno in modo che gli esperti delle prestazioni di archiviazione possano tracciare le metriche delle prestazioni utilizzando software di terze parti. Vengono visualizzate le seguenti opzioni:

- **Visualizza configurazione server:** visualizza le impostazioni di connessione e configurazione correnti per un fornitore di dati esterno.
- **Aggiungi/Modifica connessione server:** consente di immettere nuove impostazioni di connessione per un fornitore di dati esterno o di modificare le impostazioni esistenti.
- **Modifica configurazione server:** consente di immettere nuove impostazioni di configurazione per un fornitore di dati esterno o di modificare le impostazioni esistenti.
- **Elimina connessione al server:** elimina la connessione a un fornitore di dati esterno.

Dopo l'eliminazione della connessione, Unified Manager perde la connessione al server esterno.

- **Backup e ripristino**

Per informazioni, vedere gli argomenti sotto "[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 sulle prestazioni dai cluster. L'intervallo di raccolta predefinito è di 5 minuti.

È possibile modificare questo intervallo a 10 o 15 minuti se si nota 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 dell'host alla porta MySQL predefinita 3306. Per motivi di sicurezza, l'accesso tramite questa porta è limitato solo a localhost 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 localhost e host remoti, ovvero, se è abilitata solo per localhost nel tuo ambiente, puoi rendere questa porta disponibile anche per gli host remoti. In alternativa, se abilitata per tutti gli host, è possibile limitare l'accesso a questa porta solo a localhost. Se in precedenza l'accesso era abilitato sugli host remoti, la configurazione viene mantenuta in uno scenario di aggiornamento. Dopo aver attivato la visibilità della porta, è necessario controllare le impostazioni del firewall sui sistemi Windows e disattivare le impostazioni del firewall se sono configurate per limitare l'accesso alla porta MySQL 3306.

- **Uscita**

Esce dal menu della console di manutenzione.

Cambiare la password dell'utente di manutenzione su Windows

È possibile modificare la password dell'utente addetto alla manutenzione di Unified Manager quando necessario.

Passi

1. Dalla pagina di accesso dell'interfaccia utente Web di Unified Manager, fare clic su **Password dimenticata**.

Viene visualizzata una pagina in cui viene richiesto il nome dell'utente di cui si desidera reimpostare la password.

2. Inserisci il nome utente e clicca su **Invia**.

Un'e-mail con un collegamento per reimpostare la password verrà inviata all'indirizzo e-mail definito per quel nome utente.

3. Fare clic sul **link per reimpostare la password** nell'e-mail e definire la nuova password.
4. Torna all'interfaccia utente Web e accedi a Unified Manager utilizzando la nuova password.

Cambiare la password umadmin sui sistemi Linux

Per motivi di sicurezza, è necessario modificare la password predefinita per l'utente umadmin di Unified Manager subito dopo aver completato il processo di installazione. Se necessario, potrai modificare la password in qualsiasi momento successivo.

Prima di iniziare

- Unified Manager deve essere installato su un sistema Linux Red Hat Enterprise Linux.
- È necessario disporre delle credenziali utente root per il sistema Linux su cui è installato Unified Manager.

Passi

1. Accedere come utente root al sistema Linux su cui è in esecuzione Unified Manager.
2. Cambia la password umadmin:

```
passwd umadmin
```

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

Modifica le 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.

Prima di iniziare

Per accedere alla console di manutenzione del server Unified Manager è necessario disporre di un ID utente e di una password autorizzati.



Ci sono alcune porte considerate non sicure quando si utilizzano i browser Mozilla Firefox o Google Chrome. Prima di assegnare un nuovo numero di porta per il traffico HTTP e HTTPS, verifica con il tuo browser. Selezionando una porta non sicura il sistema potrebbe risultare inaccessibile e in tal caso sarebbe necessario contattare l'assistenza clienti per risolvere il problema.

L'istanza di Unified Manager viene riavviata automaticamente dopo aver modificato la porta, quindi assicurati che sia il momento giusto per disattivare il sistema per un breve periodo di tempo.

1. Accedere tramite SSH come utente di manutenzione all'host Unified Manager.

Vengono visualizzati i prompt della console di manutenzione di Unified Manager.

2. Digitare il numero dell'opzione di menu denominata **Visualizza/Modifica porte applicazione**, quindi premere Invio.
3. Se richiesto, immettere nuovamente la password dell'utente addetto alla manutenzione.
4. Digitare i nuovi numeri di porta per le porte HTTP e HTTPS, quindi premere Invio.

Lasciando vuoto il numero di porta si assegna la porta predefinita per il protocollo.

Ti verrà chiesto se desideri 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://host.company.com:1234/) , <https://12.13.14.15:1122> o [https://\[2001:db8:0:1\]:2123](https://[2001:db8:0:1]:2123).

Aggiungere interfacce di rete

È possibile aggiungere nuove interfacce di rete se è necessario separare il traffico di rete.

Prima di iniziare

È necessario aver aggiunto l'interfaccia di rete all'appliance virtuale tramite 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.

Passi

1. Nel menu principale della console vSphere, selezionare **Configurazione di sistema > Riavvia 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 **Configurazione di rete > Abilita interfaccia di rete**.
4. Selezionare la nuova interfaccia di rete e premere **Invio**.

Selezionare **eth1** e premere **Invio**.

5. Digitare **y** per abilitare l'interfaccia di rete.
6. Inserisci le impostazioni di rete.

Se si utilizza un'interfaccia statica o se non viene rilevato DHCP, verrà richiesto di immettere le impostazioni di rete.

Dopo aver inserito le impostazioni di rete, si torna automaticamente al menu **Configurazione di rete**.

7. Seleziona **Applica modifiche**.

È necessario confermare le modifiche per aggiungere l'interfaccia di rete.

Aggiungere spazio su disco alla directory del database Unified Manager

La directory del database Unified Manager contiene tutti i dati sullo stato e sulle prestazioni raccolti dai sistemi ONTAP . In alcune circostanze potrebbe essere necessario aumentare le dimensioni della directory del database.

Ad esempio, la directory del database potrebbe riempirsi se Unified Manager raccoglie dati da un numero elevato di cluster, ognuno dei quali ha molti nodi. Riceverai un evento di 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 dati sono diversi a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, su un server Red Hat o su un server Microsoft Windows.

Aggiungere spazio alla directory dati dell'host Linux

Se hai assegnato spazio su disco insufficiente al `/opt/netapp/data` directory per supportare Unified Manager quando hai originariamente configurato l'host Linux e poi installato Unified Manager, puoi aggiungere spazio su disco dopo l'installazione aumentando lo spazio su disco su `/opt/netapp/data` elenco.

Prima di iniziare

È necessario disporre dell'accesso come utente root al computer Red Hat Enterprise 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.

Passi

1. Accedi come utente root al computer Linux su cui desideri aggiungere spazio su disco.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine mostrato:

```
systemctl stop ocieau ocie mysqld
```

3. Creare una cartella di backup temporanea (ad esempio, /backup-data) con spazio su disco sufficiente a contenere i dati nella versione corrente /opt/netapp/data elenco.
4. Copia 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 SE Linux è abilitato:

- a. Ottieni il tipo 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 alla seguente:

```
echo $se_type  
mysqld_db_t
```

- a. Eseguire il comando chcon per impostare il tipo SE Linux per la directory di backup:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Rimuovere il contenuto del /opt/netapp/data elenco:

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

7. Espandi le dimensioni del /opt/netapp/data directory a un minimo di 150 GB tramite comandi LVM o aggiungendo dischi extra.



Se hai creato /opt/netapp/data da un disco, allora non dovresti provare a montarlo /opt/netapp/data come quota NFS o CIFS. Perché, in questo caso, se si tenta di espandere lo spazio su disco, alcuni comandi LVM, come `resize` E `extend` potrebbe non funzionare come previsto.

8. Confermare 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 alla seguente:

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. Se SE Linux è abilitato, confermare che il contesto per /opt/netapp/data la directory è ancora impostata su mysql_d_b_t:

a. touch /opt/netapp/data/abc

b. ls -Z /opt/netapp/data/abc

Il sistema restituisce una conferma simile alla seguente:

```
-rw-r--r--. root root unconfined_u:object_r:mysql_d_b_t:s0  
/opt/netapp/data/abc
```

10. Eliminare il file abc in modo che questo file estraneo non causi un errore del database in futuro.

11. Copia il contenuto dai dati di backup all'espanso /opt/netapp/data elenco:

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

12. Se SE Linux è abilitato, eseguire il seguente comando:

```
chcon -R --type=mysql_d_b_t /opt/netapp/data
```

13. Avviare il servizio MySQL:

```
systemctl start mysqld
```

14. Dopo aver avviato il servizio MySQL, avviare i servizi ocie e ocieau nell'ordine mostrato:

```
systemctl start ocie ocieau
```

15. Dopo aver avviato tutti i servizi, eliminare la cartella di backup /backup-data :

```
rm -rf /backup-data
```

Aggiungere 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 tramite la console di manutenzione di Unified Manager.

Prima di iniziare

- È necessario avere accesso a vSphere Client.

- La macchina virtuale non deve avere snapshot archiviati 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.

Passi

1. Nel client vSphere, seleziona la macchina virtuale Unified Manager, quindi aggiungi più capacità del disco ai dati `disk 3`. Per maggiori dettagli, consultare la documentazione VMware.

In alcuni rari casi la distribuzione di Unified Manager utilizza "Hard Disk 2" per il disco dati anziché "Hard Disk 3". Se questo si è verificato nella distribuzione, aumentare lo spazio del disco più grande. Il disco dati avrà sempre più spazio rispetto all'altro disco.

2. Nel client vSphere, seleziona la macchina virtuale Unified Manager, quindi seleziona la scheda **Console**.
3. Fare clic nella finestra della console, quindi accedere alla console di manutenzione utilizzando il nome utente e la password.
4. Nel menu principale, immettere il numero per l'opzione **Configurazione del sistema**.
5. Nel menu Configurazione di sistema, immettere il numero per l'opzione **Aumenta dimensione disco dati**.

Aggiungere 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.

Prima di iniziare

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.

Passi

1. Accedi come amministratore al server Windows su cui desideri aggiungere spazio su disco.
2. Segui il passaggio che corrisponde al metodo che vuoi utilizzare per aggiungere più spazio:

Opzione	Descrizione
Su un server fisico, aggiungere capacità all'unità logica su cui è installato il server Unified Manager.	Seguire i passaggi indicati nell'argomento Microsoft: "Estendi un volume di base"
Su un server fisico, aggiungere un'unità disco rigido.	Seguire i passaggi indicati nell'argomento Microsoft: "Aggiunta di unità disco rigido"
Su una macchina virtuale, aumentare le dimensioni di una partizione del disco.	Seguire i passaggi descritti nell'argomento VMware: "Aumento delle dimensioni di una partizione del disco"

Gestisci l'accesso degli utenti

È possibile creare ruoli e assegnare capacità per controllare l'accesso degli utenti ad Active IQ Unified Manager. È possibile identificare gli utenti che dispongono delle capacità richieste per accedere agli oggetti selezionati all'interno di Unified Manager. Solo gli utenti che dispongono di questi ruoli e capacità possono gestire gli oggetti in Unified Manager.

Aggiungi utenti

È possibile aggiungere utenti locali o utenti del database utilizzando la pagina Utenti. È anche possibile aggiungere utenti o gruppi remoti che appartengono 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 di archiviazione e i dati con Unified Manager oppure visualizzare i dati in un database.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione.
- Per aggiungere un utente o un gruppo remoto, è necessario aver abilitato l'autenticazione remota e configurato il server di autenticazione.
- Se si intende configurare l'autenticazione SAML in modo che un provider di identità (IdP) autentichi gli utenti che accedono all'interfaccia grafica, assicurarsi che tali utenti siano definiti come utenti "remoti".

L'accesso all'interfaccia utente non è consentito agli utenti di tipo "local" o "maintenance" quando è abilitata l'autenticazione SAML.

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 disabilitati. Se si aggiunge un gruppo da OpenLDAP o da altri servizi di autenticazione, solo i membri diretti di quel gruppo potranno autenticarsi in Unified Manager.

Passi

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, seleziona il tipo di utente che desideri aggiungere e inserisci le informazioni richieste.

Quando si immettono le informazioni utente richieste, è necessario specificare un indirizzo e-mail univoco per quell'utente. È necessario evitare di specificare indirizzi e-mail condivisi da più utenti.

4. Fare clic su **Aggiungi**.

Creare un utente del database

Per supportare una connessione tra Workflow Automation e Unified Manager o per accedere alle viste del database, è necessario prima creare un utente del database con il ruolo Schema di integrazione o Schema di report nell'interfaccia utente Web di Unified Manager.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Gli utenti del database forniscono l'integrazione con Workflow Automation e l'accesso a viste del database specifiche per 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.

Passi

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, seleziona **Utente database** nell'elenco a discesa **Tipo**.
4. Digitare un nome e una password per l'utente del database.
5. Nell'elenco a discesa **Ruolo**, seleziona il ruolo appropriato.

Se sei...	Scegli questo ruolo
Collegamento di Unified Manager con l'automazione del flusso di lavoro	Schema di integrazione
Accesso ai report e ad altre viste del database	Schema del report

6. Fare clic su **Aggiungi**.

Modifica le impostazioni utente

È possibile modificare le impostazioni utente, come l'indirizzo email e il ruolo, specificate per ciascun utente. Ad esempio, potresti voler modificare il ruolo di un utente che è un operatore di archiviazione e assegnare all'utente privilegi di amministratore di archiviazione.

Prima di iniziare

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 accede nuovamente a Unified Manager.
- È stato raggiunto il timeout di 24 ore della sessione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Utenti**.
2. Nella pagina Utenti, seleziona l'utente per il quale desideri modificare le impostazioni e fai clic su **Modifica**.
3. Nella finestra di dialogo Modifica utente, modificare le impostazioni appropriate specificate per l'utente.
4. Fare clic su **Salva**.

Visualizza utenti

È possibile utilizzare la pagina Utenti per visualizzare l'elenco degli utenti che gestiscono oggetti di archiviazione e dati tramite Unified Manager. È possibile visualizzare i dettagli sugli utenti, come il nome utente, il tipo di utente, l'indirizzo e-mail e il ruolo assegnato agli utenti.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Fare un passo

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Utenti**.

Elimina 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 anche possibile eliminare gruppi in modo che tutti gli utenti del gruppo non possano più accedere al server di gestione.

Prima di iniziare

- 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 rimossi.

- È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Utenti**.
2. Nella pagina Utenti, seleziona gli utenti o i gruppi che desideri eliminare, quindi fai clic su **Elimina**.
3. Fare clic su **Sì** per confermare l'eliminazione.

Che cosa è RBAC

RBAC (controllo degli accessi basato sui ruoli) offre la possibilità di controllare chi ha accesso a varie funzionalità e risorse nel server Active IQ Unified Manager .

Cosa fa il controllo degli accessi basato sui ruoli

Il controllo degli accessi basato sui ruoli (RBAC) consente agli amministratori di gestire gruppi di utenti definendo i ruoli. Se è necessario limitare l'accesso a funzionalità specifiche ad amministratori selezionati, è necessario configurare per loro degli account amministratore. Se si desidera limitare le informazioni che gli amministratori possono visualizzare e le operazioni che possono eseguire, è necessario applicare ruoli agli account amministratore creati.

Il server di gestione utilizza RBAC per l'accesso degli utenti e le autorizzazioni dei ruoli. Se non hai modificato le impostazioni predefinite del server di gestione per l'accesso degli utenti amministrativi, 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 accedere con l'account di amministratore dell'applicazione.

Definizioni dei tipi di utente

Un tipo di utente specifica il tipo di account di cui l'utente è titolare 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 addetto alla manutenzione**

Creato durante la configurazione iniziale di Unified Manager. L'utente addetto alla manutenzione crea quindi altri utenti e assegna loro i ruoli. L'utente addetto alla manutenzione è anche l'unico ad avere accesso alla console di manutenzione. Quando Unified Manager è installato su un sistema Red Hat Enterprise Linux, all'utente addetto alla manutenzione viene assegnato il nome utente "umadmin."

- **Utente locale**

Accede all'interfaccia utente di Unified Manager ed esegue funzioni in base al ruolo assegnato dall'utente addetto alla manutenzione o da un utente con il ruolo di amministratore dell'applicazione.

- **Gruppo remoto**

Un 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 sul 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 svolgere funzioni in base ai ruoli assegnati.

- **Utente remoto**

Accede all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate sul server di autenticazione. Un utente remoto esegue funzioni in base al ruolo assegnato dall'utente addetto alla manutenzione o da un utente con il ruolo di amministratore dell'applicazione.

- **Utente del database**

Ha 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 determinati privilegi. L'ambito delle attività che puoi svolgere in Unified Manager dipende dal ruolo che ti è stato assegnato e dai privilegi che il ruolo contiene.

Unified Manager include i seguenti ruoli utente predefiniti:

- **Operatore**

Visualizza le informazioni sul sistema di archiviazione e altri dati raccolti da Unified Manager, tra cui cronologie e tendenze della capacità. Questo ruolo consente all'operatore di archiviazione di visualizzare, assegnare, riconoscere, risolvere e aggiungere note per gli eventi.

- **Amministratore di archiviazione**

Configura le operazioni di gestione dell'archiviazione all'interno di Unified Manager. Questo ruolo consente all'amministratore dell'archiviazione di configurare soglie e di creare avvisi e altre opzioni e policy specifiche per la gestione dell'archiviazione.

- **Amministratore dell'applicazione**

Configura le impostazioni non correlate alla gestione dell'archiviazione. Questo ruolo consente la gestione degli utenti, dei certificati di sicurezza, dell'accesso al database e delle 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 denominato "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 del report**

Questo ruolo consente l'accesso in sola lettura ai report e ad altre visualizzazioni del database direttamente dal database Unified Manager. I database che possono essere consultati includono:

- netapp_model_view
- prestazioni netapp
- ocum
- ocum_report
- ocum_report_birt
- opm
- monitor di scala

Ruoli e capacità degli utenti di Unified Manager

In base al ruolo utente assegnato, puoi determinare quali operazioni puoi eseguire in Unified Manager.

Nella tabella seguente sono riportate le funzioni che ciascun ruolo utente può svolgere:

Funzione	Operatore	Amministratore di archiviazione	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Visualizza le informazioni sul sistema di archiviazione	•	•	•	•	•
Visualizza altri dati, come cronologie e tendenze della capacità	•	•	•	•	•
Visualizza, assegna e risolvi gli eventi	•	•	•		
Visualizza gli oggetti del servizio di archiviazione, come le associazioni SVM e i pool di risorse	•	•	•		
Visualizza le policy di soglia	•	•	•		
Gestire gli oggetti del servizio di archiviazione, come le associazioni SVM e i pool di risorse		•	•		
Definisci avvisi		•	•		
Gestisci le opzioni di gestione dell'archiviazione		•	•		

Funzione	Operatore	Amministratore di archiviazione	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Gestire le policy di gestione dell'archiviazione		•	•		
Gestisci utenti			•		
Gestisci le opzioni amministrative			•		
Definire le politiche di soglia			•		
Gestire l'accesso al database			•		
Gestire l'integrazione con WFA e fornire l'accesso alle viste del database				•	
Pianifica e salva i report		•	•		
Eseguire le operazioni "Fix It" dalle azioni di gestione		•	•		
Fornire accesso in sola lettura alle viste del database					•

Gestisci le impostazioni di autenticazione SAML

Dopo aver configurato le impostazioni di autenticazione remota, è possibile abilitare 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.

Si noti che solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo aver

abilitato l'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non ha alcun impatto sugli utenti che accedono alla console di manutenzione.

Requisiti del fornitore 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 richieste affinché la connessione a Unified Manager abbia successo.

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 fornitore di servizi (SP) nello standard Security Assertion Markup Language (SAML).

Standard di crittografia supportati

- Standard di crittografia avanzata (AES): AES-128 e AES-256
- Algoritmo hash sicuro (SHA): SHA-1 e SHA-256

Fornitori di identità convalidati

- Shibboleth
- Servizi federativi di Active Directory (ADFS)

Requisiti di configurazione ADFS

- È necessario definire tre regole di attestazione nel seguente ordine, necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della relying party.

Regola di rivendicazione	Valore
Nome account SAM	ID nome
Nome account SAM	urna:oid:0.9.2342.19200300.100.1.1
Gruppi di token — Nome non qualificato	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- È necessario impostare il metodo di autenticazione su "Autenticazione tramite moduli" altrimenti gli utenti potrebbero ricevere un errore quando escono da Unified Manager. Segui questi passaggi:
 - a. Aprire la console di gestione ADFS.
 - b. Fare clic sulla cartella Criteri di autenticazione nella vista ad albero a sinistra.
 - c. In Azioni sulla destra, fare clic su Modifica criterio di autenticazione primaria globale.
 - d. Impostare il metodo di autenticazione Intranet su "Autenticazione basata su moduli" anziché sul valore predefinito "Autenticazione Windows".
- In alcuni casi l'accesso tramite IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato da una CA. Esistono due soluzioni alternative per risolvere questo problema:
 - Seguire le istruzioni identificate nel collegamento per disattivare il controllo di revoca sul server ADFS

per la parte affidabile associata al certificato CA concatenato:

"Disabilita il controllo di revoca per trust della parte affidabile"

- Fare in modo che il server CA risieda all'interno del server ADFS per firmare la richiesta di certificato del server Unified Manager.

Altri requisiti di configurazione

- Lo sfasamento dell'orologio di Unified Manager è impostato su 5 minuti, quindi la differenza di orario tra il server IdP e il server Unified Manager non può essere superiore a 5 minuti, altrimenti l'autenticazione fallirà.

Abilita l'autenticazione SAML

È possibile abilitare 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.

Prima di iniziare

- È necessario aver configurato l'autenticazione remota e verificato che sia andata a buon fine.
- 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 e dei metadati dell'IdP.
- È necessario avere accesso al server IdP.

Dopo aver abilitato l'autenticazione SAML da Unified Manager, gli utenti non potranno accedere all'interfaccia utente grafica finché l'IdP non sarà stato configurato con le informazioni sull'host del server Unified Manager. Pertanto, prima di iniziare il processo di configurazione, è necessario essere pronti a completare entrambe le parti della connessione. 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 aver abilitato l'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non ha alcun impatto 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione SAML**.
2. Selezionare la casella di controllo **Abilita autenticazione SAML**.

Vengono visualizzati i campi necessari per configurare la connessione IdP.

3. Immettere l'URI IdP e i metadati IdP necessari 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 **Recupera metadati IdP** dopo aver immesso l'URI IdP per popolare automaticamente il campo Metadati IdP.

4. Copiare l'URI dei metadati dell'host Unified Manager oppure salvare i metadati dell'host in un file di testo XML.

È possibile configurare il server IdP con queste informazioni in questo momento.

5. Fare clic su **Salva**.

Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

6. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.

La prossima volta che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso dell'IdP anziché nella pagina di accesso di Unified Manager.

Se non è ancora stato fatto, accedi al tuo IdP e inserisci l'URI e i metadati del server Unified Manager per completare la configurazione.



Quando si utilizza ADFS come provider di identità, l'interfaccia utente grafica di Unified Manager non rispetta il timeout di ADFS e continuerà a funzionare finché non verrà raggiunto il timeout della sessione di Unified Manager. È possibile modificare il timeout della sessione GUI facendo clic su **Generale > Impostazioni funzionalità > Timeout di inattività**.

Cambia il 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.

Prima di iniziare

- È necessario disporre dell'URL e dei metadati dell'IdP.
- È necessario avere accesso all'IdP.

Il nuovo IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione SAML**.
2. Immettere il nuovo URI IdP e i metadati IdP necessari per connettere il server Unified Manager all'IdP.

Se l'IdP è accessibile direttamente dal server Unified Manager, è possibile fare clic sul pulsante **Recupera metadati IdP** dopo aver immesso l'URL dell'IdP per popolare automaticamente il campo Metadati IdP.

3. Copiare l'URI dei metadati di Unified Manager oppure salvare i metadati in un file di testo XML.
4. Fare clic su **Salva configurazione**.

Viene visualizzata una finestra di messaggio per confermare che si desidera modificare la configurazione.

5. Fare clic su **OK**.

Accedi al nuovo IdP e inserisci l'URI e i metadati del server Unified Manager per completare la configurazione.

La prossima volta 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.

Aggiorna le impostazioni di autenticazione SAML dopo la modifica del certificato di sicurezza di Unified Manager

Qualsiasi modifica al certificato di sicurezza HTTPS installato sul server Unified Manager richiede l'aggiornamento delle impostazioni di configurazione dell'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 sicurezza per il sistema.

Dopo aver modificato il certificato di sicurezza e riavviato il server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non saranno in grado di accedere all'interfaccia grafica di Unified Manager. È necessario aggiornare le impostazioni di autenticazione SAML sia sul server IdP che sul server Unified Manager per riabilitare l'accesso all'interfaccia utente.

Passi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, immettere il numero per l'opzione **Disabilita autenticazione SAML**.

Viene visualizzato un messaggio per confermare che si desidera disabilitare 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 ed effettuare l'accesso utilizzando le credenziali dell'utente addetto alla manutenzione.
4. Nella pagina **Configurazione/Autenticazione**, seleziona la scheda **Autenticazione SAML** e configura la connessione IdP.
5. Copiare l'URI dei metadati dell'host Unified Manager oppure salvare i metadati dell'host in un file di testo XML.
6. Fare clic su **Salva**.

Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

7. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.
8. Accedi al tuo server IdP e inserisci l'URI e i metadati del server Unified Manager per completare la configurazione.

Fornitore di identità	Fasi di configurazione
ADFS	a. Eliminare la voce di trust della relying party esistente nell'interfaccia utente grafica di gestione ADFS. b. Aggiungere una nuova voce di trust della parte affidabile utilizzando <code>saml_sp_metadata.xml</code> dal server Unified Manager aggiornato. c. Definire le tre regole di claim necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della relying party. d. Riavviare il servizio ADFS di Windows.
Shibboleth	a. Aggiorna il nuovo FQDN del server Unified Manager in <code>attribute-filter.xml</code> E <code>relying-party.xml</code> file. b. Riavviare il server web Apache Tomcat e attendere che la porta 8005 torni online.

9. Accedi a Unified Manager e verifica che l'autenticazione SAML funzioni come previsto tramite il tuo IdP.

Disabilitare l'autenticazione SAML

È possibile disabilitare 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 disabilitata, i provider di servizi di directory configurati, come Active Directory o LDAP, eseguono l'autenticazione di accesso.

Dopo aver disabilitato l'autenticazione SAML, gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica, oltre agli utenti remoti configurati.

È anche possibile disabilitare l'autenticazione SAML tramite la console di manutenzione di Unified Manager se non si ha accesso all'interfaccia utente grafica.



Unified Manager viene riavviato automaticamente dopo aver disabilitato l'autenticazione SAML.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione SAML**.
2. Deseleziona la casella di controllo **Abilita autenticazione SAML**.
3. Fare clic su **Salva**.

Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

4. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.

La prossima volta 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 dell'IdP.

Accedi al tuo IdP ed elimina l'URI e i metadati del server Unified Manager.

Disabilitare l'autenticazione SAML dalla console di manutenzione

Potrebbe essere necessario disabilitare l'autenticazione SAML dalla console di manutenzione quando non è possibile accedere all'interfaccia utente grafica di Unified Manager. Ciò potrebbe verificarsi in caso di configurazione errata o se l'IdP non è accessibile.

Prima di iniziare

È necessario avere accesso alla console di manutenzione come utente addetto alla manutenzione.

Quando l'autenticazione SAML è disabilitata, i provider di servizi di directory configurati, come Active Directory o LDAP, eseguono l'autenticazione di accesso. Oltre agli utenti remoti configurati, gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica.

È anche possibile disabilitare l'autenticazione SAML dalla pagina Configurazione/Autenticazione nell'interfaccia utente.



Unified Manager viene riavviato automaticamente dopo aver disabilitato l'autenticazione SAML.

Passi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, immettere il numero per l'opzione **Disabilita autenticazione SAML**.

Viene visualizzato un messaggio per confermare che si desidera disabilitare l'autenticazione SAML e riavviare Unified Manager.

3. Digitare **y**, quindi premere Invio; Unified Manager verrà riavviato.

La prossima volta 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 dell'IdP.

Se necessario, accedi al tuo IdP ed elimina l'URL e i metadati del server Unified Manager.

Pagina di autenticazione SAML

È possibile utilizzare la pagina Autenticazione SAML per configurare Unified Manager in modo che autentichi gli utenti remoti tramite 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, è possibile selezionare la casella di controllo **Abilita autenticazione SAML** per abilitare l'autenticazione tramite un provider di identità sicuro.

- **URI IdP**

L'URI per accedere all'IdP dal server Unified Manager. Di seguito sono elencati alcuni esempi di URI.

URI di esempio ADFS:

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Esempio di URI di Shibboleth:

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **Metadati IdP**

Metadati IdP in formato XML.

Se l'URL dell'IdP è accessibile dal server Unified Manager, è possibile fare clic sul pulsante **Recupera metadati IdP** per popolare questo campo.

- **Sistema host (FQDN)**

FQDN del sistema host Unified Manager come definito durante l'installazione. Se necessario, è possibile modificare questo valore.

- **URI host**

L'URI per accedere al sistema host Unified Manager dall'IdP.

- **Metadati host**

Metadati del sistema host in formato XML.

Gestisci l'autenticazione

È possibile abilitare l'autenticazione tramite LDAP o Active Directory sul server Unified Manager e configurarlo in modo che funzioni con i server per autenticare gli 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 i server di autenticazione

È possibile modificare la porta utilizzata dal server Unified Manager per comunicare con il server di autenticazione.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Selezionare la casella **Disabilita ricerca gruppi annidati**.
3. Nell'area **Server di autenticazione**, seleziona il server di autenticazione che desideri modificare, quindi fai clic su **Modifica**.
4. Nella finestra di dialogo **Modifica server di autenticazione**, modificare i dettagli della porta.
5. Fare clic su **Salva**.

Elimina i 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 comunica il server di gestione, è possibile eliminare il server di autenticazione e aggiungerne uno nuovo.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Quando si elimina un server di autenticazione, gli utenti o i gruppi remoti del server di autenticazione non saranno più in grado di accedere a Unified Manager.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Selezionare uno o più server di autenticazione che si desidera eliminare, quindi fare clic su **Elimina**.
3. Fare clic su **Sì** per confermare la richiesta di eliminazione.

Se l'opzione **Usa connessione protetta** è abilitata, i certificati associati al server di autenticazione vengono eliminati insieme al server di autenticazione.

Autenticazione con Active Directory o OpenLDAP

È possibile abilitare 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 oppure specificare un proprio servizio di autenticazione:

- 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 gli utenti o i gruppi remoti sono 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 di controllo

È possibile rilevare se i registri di controllo sono stati compromessi utilizzando i registri di controllo. Tutte le attività svolte da un utente vengono monitorate e registrate nei registri di controllo. Gli audit vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API esposte pubblicamente di Active IQ Unified Manager.

È possibile utilizzare **Registro di controllo: Visualizzazione file** per visualizzare e accedere a tutti i file del registro di controllo disponibili in Active IQ Unified Manager. I file nel Registro di controllo: Visualizzazione file sono elencati in base alla data di creazione. Questa vista mostra le informazioni di tutti i registri di controllo acquisiti dall'installazione o dall'aggiornamento fino al momento 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 registro viene acquisito tramite l'attributo "File Integrity Status", che viene monitorato attivamente per rilevare manomissioni o eliminazioni del file di registro. Quando sono disponibili nel sistema, i registri di controllo possono avere uno dei seguenti stati:

Stato	Descrizione
ATTIVO	File in cui vengono attualmente registrati i log.
NORMALE	File inattivo, compresso e memorizzato nel sistema.
MANOMESTRI	File compromesso da un utente che lo ha modificato manualmente.
ELIMINA_MANUALE	File eliminato da un utente autorizzato.
ROLLOVER_ELIMINA	File eliminato a causa del roll-off basato sulla politica di configurazione rolling.
ELIMINAZIONE_INATTESA	File eliminato per motivi sconosciuti.

La pagina Registro di controllo include i seguenti pulsanti di comando:

- Configurare
- Eliminare
- Scaricamento

Il pulsante **ELIMINA** consente di eliminare uno qualsiasi dei registri di controllo elencati nella vista Registri di controllo. È possibile eliminare un registro di controllo e, facoltativamente, specificare un motivo per eliminare il file, che aiuterà in futuro a determinare un'eliminazione valida. Nella colonna MOTIVO è elencato il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.



L'eliminazione di un file di registro comporterà l'eliminazione del file dal sistema, ma la voce nella tabella del database 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 come "NORMALI" o "MANOMESSI" vengono scaricati in un formato compresso .gzip formato.

I file di registro di controllo vengono archiviati periodicamente e salvati nel database per riferimento. Prima dell'archiviazione, i registri di controllo vengono firmati digitalmente per garantirne la sicurezza e l'integrità.

Quando viene generato un bundle AutoSupport completo, il bundle di supporto include sia i file di registro di controllo archiviati che quelli attivi. Tuttavia, quando viene generato un pacchetto di supporto leggero, include solo i log di controllo attivi. I registri di controllo archiviati non sono inclusi.

Configurare i registri di controllo

È possibile utilizzare il pulsante **Configura** nella sezione Registri di controllo per configurare la policy di rotazione per i file dei registri di controllo e per abilitare anche la registrazione remota per i registri di controllo.

È possibile impostare i valori in **DIMENSIONE MASSIMA FILE** e **GIORNI DI CONSERVAZIONE REGISTRO DI CONTROLLO** in base alla quantità e alla frequenza desiderate dei dati che si desidera archiviare nel sistema. Il valore nel campo **DIMENSIONE TOTALE REGISTRO DI CONTROLLO** è la dimensione totale dei dati del registro di controllo presenti nel sistema. La politica di rollover è determinata dai valori nei campi **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO**, **DIMENSIONE MASSIMA DEL FILE** e **DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO**. Quando la dimensione del backup del registro di controllo raggiunge il valore configurato in **DIMENSIONE TOTALE REGISTRO DI CONTROLLO**, il file archiviato per primo viene eliminato. Ciò significa che il file più vecchio viene eliminato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Eliminazione rollover". Il valore **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO** indica il numero di giorni in cui vengono conservati i file del registro di controllo. Tutti i file più vecchi del valore impostato in questo campo vengono riportati al valore precedente.

Passi

1. Fare clic su **Registri di controllo > > Configura**.
2. Immettere i valori in **DIMENSIONE MASSIMA DEL FILE**, **DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO** e **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO**.

Se si desidera abilitare la registrazione remota, è necessario selezionare **Abilita registrazione remota**. ///
2025-6-11, OTHERDOC-133

Abilita la registrazione remota dei log di controllo

È possibile selezionare la casella di controllo **Abilita registrazione remota** nella finestra di dialogo Configura registri di controllo per abilitare la registrazione di controllo remota. È possibile utilizzare questa funzionalità per trasferire i registri di controllo a un server Syslog remoto. Ciò ti consentirà di gestire i registri di controllo quando ci sono vincoli di spazio.

La registrazione remota dei registri di controllo fornisce un backup a prova di manomissione nel caso in cui i file del registro di controllo sul server Active IQ Unified Manager vengano manomessi.

Passi

1. Nella finestra di dialogo **Configura registri di controllo**, selezionare la casella di controllo **Abilita registrazione remota**.

Vengono visualizzati campi aggiuntivi per configurare la registrazione remota.

2. Inserisci **HOSTNAME** e **PORT** del server remoto a cui vuoi connetterti.
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 dovrebbe contenere il nome host selezionato come parte del SubjectAltName attributo (SAN).

4. Immettere i valori per i seguenti campi: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

Per questi campi i valori devono essere espressi in millisecondi.

5. Selezionare il formato Syslog e la versione del protocollo TLS richiesti nei campi **FORMATO** e **PROTOCOLLO**.
6. Selezionare la casella di controllo **Abilita autenticazione client** se il server Syslog di destinazione richiede l'autenticazione basata su certificato.

Sarà necessario scaricare il certificato di autenticazione client e caricarlo sul server Syslog prima di salvare la configurazione del registro di controllo, altrimenti la connessione non riuscirà. A seconda del tipo di server Syslog, potrebbe essere necessario creare un hash del certificato di autenticazione client.

Esempio: syslog-ng richiede che venga creato un <hash> del certificato utilizzando il comando `openssl x509 -noout -hash -in cert.pem`, quindi dovresti collegare simbolicamente il certificato di autenticazione client a un file denominato dopo <hash> .0.

7. Fare clic su **Salva** per configurare la connessione con il server e abilitare la registrazione remota.

Verrai reindirizzato alla pagina Registri di controllo.



Il valore **Timeout connessione** può influire sulla configurazione. Se la configurazione impiega più tempo per rispondere rispetto al valore definito, potrebbe verificarsi un errore di configurazione a causa di un errore di connessione. Per stabilire una connessione riuscita, aumentare il valore **Timeout connessione** e riprovare la configurazione.

Pagina di autenticazione remota

È possibile utilizzare la pagina 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 Amministratore dell'archiviazione.

Dopo aver selezionato la casella di controllo Abilita autenticazione remota, è possibile abilitare l'autenticazione remota tramite un server di autenticazione.

- **Servizio di autenticazione**

Consente di configurare il server di gestione per autenticare gli utenti nei provider di servizi di directory, come Active Directory, OpenLDAP, oppure di specificare un proprio meccanismo di autenticazione. È possibile specificare un servizio di autenticazione solo se è stata abilitata l'autenticazione remota.

- **Directory attiva**

- Nome dell'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**.

- Disabilita la ricerca di gruppi nidificati

Specifica se abilitare o disabilitare l'opzione di ricerca dei gruppi annidati. Per impostazione predefinita questa opzione è disabilitata. Se si utilizza Active Directory, è possibile velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

- Utilizza una connessione sicura

Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

- **OpenLDAP**

- Associa nome distinto

Specifica il nome distinto di associazione utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione.

- Password di associazione

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**.

- Utilizza una connessione sicura

Specifica che Secure LDAP viene utilizzato per comunicare con i server di autenticazione LDAP.

- **Altri**

- Associa nome distinto

Specifica il nome distinto di associazione utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione configurato.

- Password di associazione

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 del protocollo LDAP (Lightweight Directory Access Protocol) supportata dal server di autenticazione. È possibile specificare se la versione del protocollo deve essere rilevata automaticamente oppure impostare la versione su 2 o 3.

- Attributo nome utente

Specifica il nome dell'attributo nel server di autenticazione che contiene i nomi di accesso utente da autenticare tramite il server di gestione.

- Attributo di appartenenza al gruppo

Specifica un valore che assegna l'appartenenza al gruppo del 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 del server di gestione agli utenti remoti in base a un attributo specificato in tale oggetto GroupOfUniqueNames.

- Disabilita la ricerca di gruppi nidificati

Specifica se abilitare o disabilitare l'opzione di ricerca dei gruppi annidati. Per impostazione predefinita questa opzione è disabilitata. Se si utilizza Active Directory, è possibile velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

- Membro

Specifica il nome dell'attributo utilizzato dal server di autenticazione per memorizzare le informazioni sui singoli membri di un gruppo.

- Classe oggetto utente

Specifica la classe di oggetti di un utente nel server di autenticazione remoto.

- Classe di oggetti di 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 essere gli stessi aggiunti nelle configurazioni di Active Directory, OpenLDAP e LDAP. In caso contrario, l'autenticazione potrebbe fallire.

- Utilizza una 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 di aggiungerne di nuovi.

Area server di autenticazione

L'area Server di autenticazione visualizza i server di autenticazione con cui il server di gestione comunica per trovare e autenticare gli utenti remoti. Le credenziali per gli utenti o i gruppi remoti sono gestite dal server di autenticazione.

• Pulsanti di comando

Consente di aggiungere, modificare o eliminare server di autenticazione.

- Aggiungere

Consente di aggiungere un server di autenticazione.

Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (che utilizza 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.

- Modificare

Consente di modificare le impostazioni per 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.

• Test di 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 cerca l'utente remoto nel server di autenticazione, ma non lo autentica. Se si specificano sia il nome utente che la password, il server di gestione cerca e autentica l'utente remoto.

Non è possibile testare l'autenticazione se l'autenticazione remota è disabilitata.

Gestire i certificati di sicurezza

È possibile configurare HTTPS nel server Unified Manager per monitorare e gestire i cluster tramite una connessione sicura.

Visualizza il certificato di sicurezza HTTPS

È possibile confrontare i dettagli del certificato HTTPS con il certificato recuperato nel browser per assicurarsi che la connessione crittografata del browser a Unified Manager non venga intercettata.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

La visualizzazione del certificato consente di verificare il contenuto di un certificato rigenerato o di visualizzare i nomi alternativi del soggetto (SAN) da cui è possibile accedere a Unified Manager.

Fare un passo

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Certificato HTTPS**.

Il certificato HTTPS viene visualizzato nella parte superiore della pagina

Se hai bisogno di visualizzare informazioni più dettagliate sul certificato di sicurezza rispetto a quelle visualizzate nella pagina Certificato HTTPS, puoi visualizzare il certificato di connessione nel tuo browser.

Scarica una richiesta di firma del certificato HTTPS

È possibile scaricare una richiesta di firma della certificazione per l'attuale certificato di sicurezza HTTPS, in modo da poter fornire il file a un'autorità di certificazione per la firma. Un certificato firmato da una CA aiuta a prevenire gli attacchi man-in-the-middle e offre una migliore protezione di sicurezza rispetto a un certificato autofirmato.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Certificato HTTPS**.
2. Fare clic su **Scarica richiesta di firma del certificato HTTPS**.
3. Salva il `<hostname>.csr` file.

È possibile fornire il file a un'autorità di certificazione affinché lo firmi e quindi installare il certificato firmato.

Installa un certificato HTTPS firmato e restituito da una CA

È possibile caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione lo ha firmato e restituito. Il file che carichi e installi deve essere una versione firmata del certificato autofirmato esistente. Un certificato firmato da una CA

aiuta a prevenire gli attacchi man-in-the-middle e fornisce una migliore protezione di sicurezza rispetto a un certificato autofirmato.

*Cosa. Prima di iniziare

Devi aver completato le seguenti azioni:

- Ho scaricato il file di richiesta di firma del certificato e l'ho fatto firmare da un'autorità di certificazione
- Salvata la catena di certificati in formato PEM
- Inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma radice, inclusi tutti i certificati intermedi presenti

È necessario disporre del ruolo di amministratore dell'applicazione.



Se la validità del certificato per il quale è stato creato un CSR è superiore a 397 giorni, la validità verrà ridotta a 397 giorni dalla CA prima di firmare e restituire il certificato

Passi

1. Nel riquadro di navigazione 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 informazioni, vedere ["Installazione di un certificato HTTPS generato tramite strumenti esterni"](#).

Esempio di catena di certificati

L'esempio seguente mostra come potrebbe apparire il file della catena di certificati:

```
-----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-----
```

Installa un certificato HTTPS generato utilizzando strumenti esterni

È possibile installare certificati autofirmati o firmati da una CA e generati tramite uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

È necessario caricare la chiave privata insieme alla catena di certificati, poiché questi certificati sono coppie di chiavi pubblica-privata 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 inverso fino alla radice, che vengono utilizzati 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-----

```

Dopo aver caricato il certificato, è necessario riavviare l'istanza di Active IQ Unified Manager affinché le modifiche abbiano effetto.

Controlli durante il caricamento di certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato tramite strumenti esterni. Se uno qualsiasi dei controlli fallisce, il certificato viene rifiutato. Sono incluse anche le convalide per i certificati generati dal CSR all'interno del prodotto e per i certificati generati tramite strumenti esterni.

- La chiave privata nell'input viene convalidata rispetto al certificato host nell'input.
- Il nome comune (CN) nel certificato host viene confrontato con l'FQDN dell'host.
- Il nome comune (CN) del certificato host non deve essere vuoto e non deve essere impostato su localhost.
- La data di inizio della validità del certificato non deve essere nel futuro e la data di scadenza della validità del certificato non deve essere nel passato.
- Se esiste una CA intermedia o una CA, la data di inizio 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-----
```

Se l'installazione del certificato non riesce, consultare l'articolo della Knowledge Base (KB):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager non riesce a installare un certificato generato esternamente"]

Descrizioni delle pagine per la gestione dei certificati

È possibile utilizzare la pagina Certificato HTTPS per visualizzare i certificati di sicurezza correnti e per generare nuovi certificati HTTPS.

Pagina del certificato HTTPS

La pagina Certificato HTTPS consente di visualizzare il certificato di sicurezza corrente, scaricare una richiesta di firma del certificato, generare un nuovo certificato HTTPS autofirmato o installare un nuovo certificato HTTPS.

Se non hai generato un nuovo certificato HTTPS autofirmato, il certificato visualizzato in questa pagina è quello generato durante l'installazione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Scarica la richiesta di firma del certificato HTTPS**

Scarica una richiesta di certificazione per il certificato HTTPS attualmente installato. Il browser ti chiede di salvare il file <hostname>.csr in modo da poterlo fornire a un'autorità di certificazione per la firma.

- **Installa il certificato HTTPS**

Consente di caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione lo ha firmato e restituito. Il nuovo certificato sarà effettivo dopo il riavvio del server di gestione.

- **Rigenera il certificato HTTPS**

Consente di generare un nuovo certificato HTTPS autofirmato, che sostituisce l'attuale certificato di sicurezza. Il nuovo certificato sarà effettivo 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 sicurezza e quindi di generare un nuovo certificato HTTPS con tali informazioni.

Le informazioni attuali sul certificato vengono visualizzate in questa pagina.

Le selezioni "Rigenera utilizzando gli attributi del certificato corrente" e "Aggiorna gli attributi del certificato corrente" consentono di rigenerare il certificato con le informazioni correnti o di generare un certificato con nuove informazioni.

- **Nome comune**

Necessario. Il nome di dominio completamente qualificato (FQDN) che desideri proteggere.

Nelle configurazioni ad alta disponibilità di Unified Manager, utilizzare l'indirizzo IP virtuale.

- **E-mail**

Opzionale. Un indirizzo email per contattare la tua organizzazione; in genere l'indirizzo email dell'amministratore del certificato o del reparto IT.

- **Azienda**

Opzionale. Solitamente è il nome della società.

- **Dipartimento**

Opzionale. Il nome del reparto della tua azienda.

- **Città**

Opzionale. La sede della tua azienda in città.

- **Stato**

Opzionale. La sede della tua azienda, non in forma abbreviata, nello stato o nella provincia.

- **Paese**

Opzionale. Il paese in cui ha sede la tua azienda. In genere si tratta di un codice ISO di due lettere del Paese.

- **Nomi alternativi**

Necessario. Nomi di dominio aggiuntivi, non primari, che possono essere utilizzati per accedere a questo server oltre all'indirizzo localhost o ad altri indirizzi di rete esistenti. Separare ogni nome alternativo con una virgola.

Selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad esempio localhost)" se si desidera rimuovere le informazioni di identificazione locali dal campo Nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi verrà utilizzato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

- **DIMENSIONE CHIAVE (ALGORITMO CHIAVE: RSA)**

L'algoritmo chiave è impostato su RSA. È possibile selezionare una delle seguenti dimensioni della chiave: 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 hai effettuato l'aggiornamento da una versione precedente, potresti notare che la validità del certificato precedente è rimasta invariata.

Per maggiori informazioni, vedere ["Generazione di certificati HTTPS"](#).

Monitorare e gestire l'archiviazione

Introduzione ad Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) consente di monitorare e gestire lo stato e le prestazioni dei sistemi di archiviazione ONTAP da un'unica interfaccia.

Unified Manager offre le seguenti funzionalità:

- Rilevamento, monitoraggio e notifiche per i sistemi installati con il software ONTAP .
- Dashboard per mostrare la capacità, la sicurezza e lo stato delle prestazioni dell'ambiente.
- Avvisi, eventi e infrastruttura di soglia migliorati.
- Visualizza grafici dettagliati che tracciano l'attività del carico di lavoro nel tempo, inclusi IOPS (operazioni), MBps (throughput), latenza (tempo di risposta), utilizzo, capacità delle prestazioni e rapporto della cache.
- Identifica i carichi di lavoro che utilizzano eccessivamente i componenti del cluster e i carichi di lavoro le cui prestazioni sono influenzate dall'aumento dell'attività.
- Fornisce suggerimenti sulle azioni correttive che possono essere eseguite per risolvere determinati incidenti ed eventi, nonché un pulsante "Risolvi" per alcuni eventi, in modo da poter risolvere immediatamente il problema.
- 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 file, direttamente da Unified Manager e di assegnare un livello di servizio delle prestazioni per definire gli obiettivi di prestazioni e archiviazione per gli utenti che accedono all'applicazione utilizzando tale carico di lavoro.

Introduzione al monitoraggio dello stato di salute Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) consente di monitorare un gran numero di sistemi che eseguono il software ONTAP tramite un'interfaccia utente centralizzata. L'infrastruttura del server Unified Manager offre scalabilità, supporto e funzionalità avanzate di monitoraggio e notifica.

Le funzionalità principali di Unified Manager includono il monitoraggio, l'invio di avvisi, la gestione della disponibilità e della capacità dei cluster, la gestione delle capacità di protezione e il raggruppamento dei dati diagnostici e il loro invio al supporto tecnico.

Puoi utilizzare Unified Manager per monitorare i tuoi cluster. Quando si verificano problemi nel cluster, Unified Manager ti informa sui dettagli di tali problemi tramite eventi. Alcuni eventi forniscono anche un'azione correttiva che puoi intraprendere per risolvere i problemi. È possibile configurare avvisi per gli eventi in modo che, quando si verificano problemi, si venga avvisati tramite e-mail e trap SNMP.

È possibile utilizzare Unified Manager per gestire gli oggetti di archiviazione nel proprio ambiente associandoli ad annotazioni. È possibile creare annotazioni personalizzate e associare dinamicamente cluster, macchine virtuali di archiviazione (SVM) e volumi alle annotazioni tramite regole.

È inoltre possibile pianificare i requisiti di archiviazione degli oggetti del cluster utilizzando le informazioni fornite nei grafici di capacità e integrità per il rispettivo oggetto del cluster.

Capacità fisica e logica

Unified Manager sfrutta i concetti di spazio fisico e logico utilizzati per gli oggetti di archiviazione ONTAP .

- Capacità fisica: lo spazio fisico si riferisce ai blocchi fisici di archiviazione utilizzati nel volume. La "capacità fisica utilizzata" è in genere inferiore alla capacità logica utilizzata a causa della riduzione dei dati derivanti dalle funzionalità di efficienza di archiviazione (come deduplicazione 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 può essere utilizzato lo spazio teorico, senza tenere conto dei risultati della deduplicazione o della compressione. Lo "spazio logico utilizzato" è lo spazio fisico utilizzato più i risparmi derivanti dalle funzionalità di efficienza di archiviazione (come deduplicazione e compressione) che sono state configurate. Questa misurazione appare spesso maggiore della capacità fisica utilizzata perché 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 di archiviazione in base a unità binarie di 1024 (2^{10}) byte. In ONTAP 9.10.0 e nelle 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 la velocità effettiva continuano a essere kilobyte al secondo (Kbps), megabyte al secondo (Mbps), gigabyte al secondo (Gbps) o terabyte al 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
tubercolosi	TiB	$1024 * 1024 * 1024 * 1024$	1.099.511.627.776 byte

Introduzione al monitoraggio delle prestazioni Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) offre funzionalità di monitoraggio delle prestazioni 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 utilizzano eccessivamente i componenti del cluster e riducono le prestazioni degli altri carichi di lavoro sul cluster. Definendo criteri di soglia delle prestazioni è anche possibile specificare valori massimi per determinati contatori delle prestazioni, in modo che vengano generati eventi quando la soglia viene superata. Unified Manager ti avvisa di questi eventi relativi alle prestazioni, in modo che tu possa adottare misure correttive e riportare le prestazioni ai normali livelli operativi.

È possibile visualizzare e analizzare gli eventi nell'interfaccia utente di Unified Manager.

Unified Manager monitora le prestazioni 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.

Utilizzare le API REST di Unified Manager

Active IQ Unified Manager fornisce API REST per visualizzare le informazioni sul monitoraggio e la gestione dell'ambiente di archiviazione. Le API consentono inoltre di effettuare il provisioning e gestire oggetti di archiviazione in base a criteri.

È inoltre possibile eseguire le API ONTAP su tutti i cluster gestiti ONTAP utilizzando il gateway API supportato da Unified Manager.

Per informazioni sulle API REST di Unified Manager, vedere ["Introduzione alle API REST Active IQ Unified Manager"](#).

Cosa fa il server Unified Manager

L'infrastruttura del server Unified Manager è composta da un'unità di raccolta dati, un database e un server applicativo. Fornisce servizi infrastrutturali quali individuazione, monitoraggio, controllo degli accessi basato sui ruoli (RBAC), auditing e registrazione.

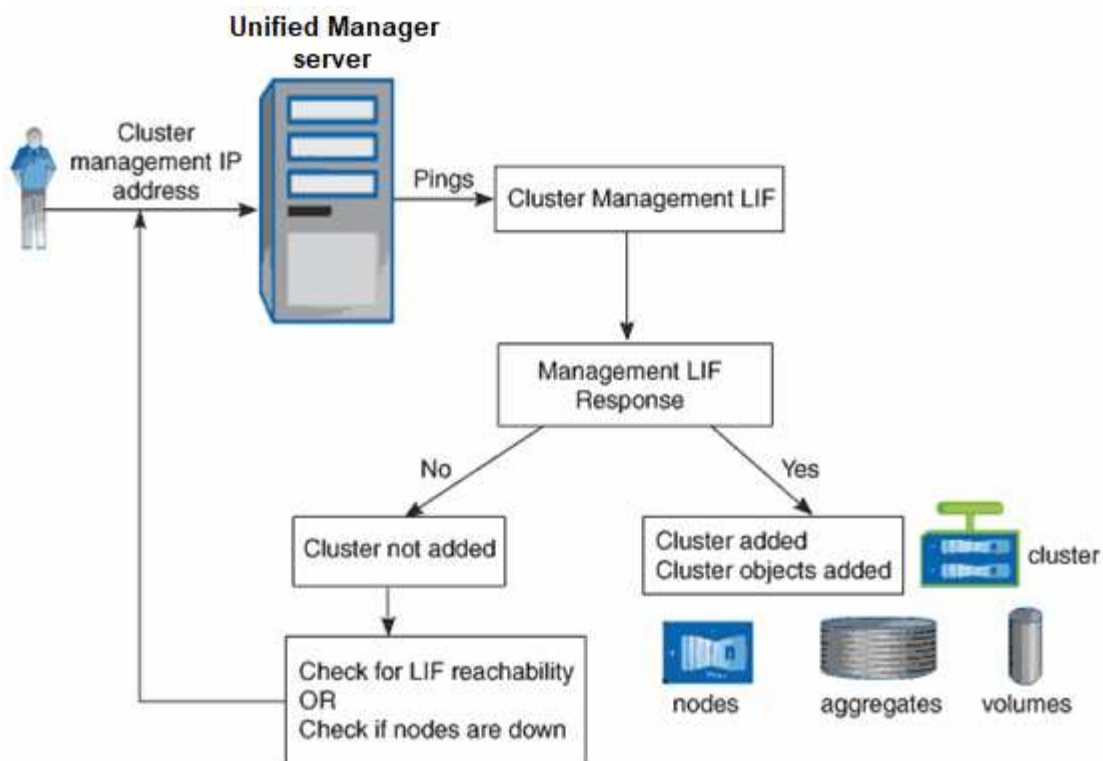
Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare se ci sono problemi nel cluster.

Come funziona il processo di scoperta

Dopo aver aggiunto il cluster a Unified Manager, il server rileva gli oggetti del cluster e li aggiunge al proprio database. Comprendere il funzionamento del processo di individuazione ti aiuta a gestire i cluster della tua organizzazione e i relativi oggetti.

L'intervallo di monitoraggio predefinito è di 15 minuti: se hai aggiunto un cluster al server Unified Manager, ci vogliono 15 minuti per visualizzare i dettagli del cluster nell'interfaccia utente di Unified Manager.

L'immagine seguente illustra il processo di individuazione in Active IQ Unified Manager:



Comprendere l'interfaccia utente

L'interfaccia utente di Unified Manager è costituita principalmente da una dashboard che fornisce una panoramica immediata degli oggetti monitorati. L'interfaccia utente consente inoltre di visualizzare tutti gli oggetti del cluster.

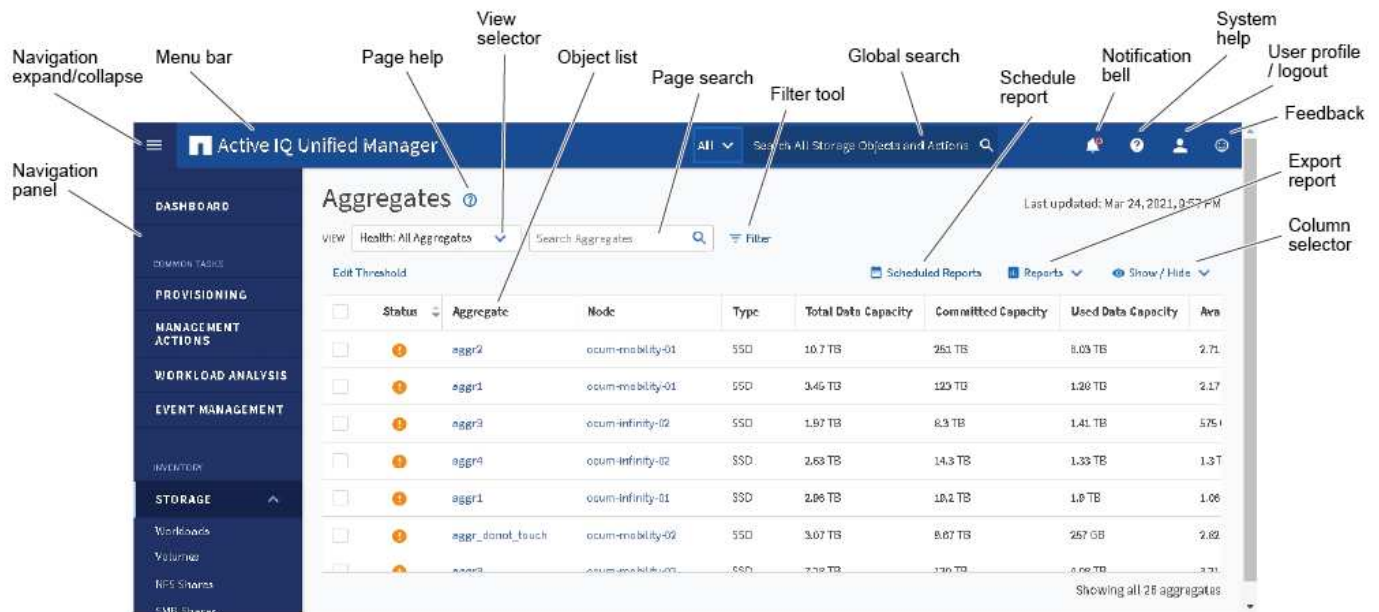
È possibile selezionare la visualizzazione preferita e utilizzare i pulsanti di azione secondo necessità. La configurazione dello schermo viene salvata in un'area di lavoro, in modo che tutte le funzionalità necessarie siano disponibili all'avvio di Unified Manager. Tuttavia, quando si passa da una vista all'altra e poi si torna indietro, la vista potrebbe non essere la stessa.

Tipiche disposizioni delle finestre

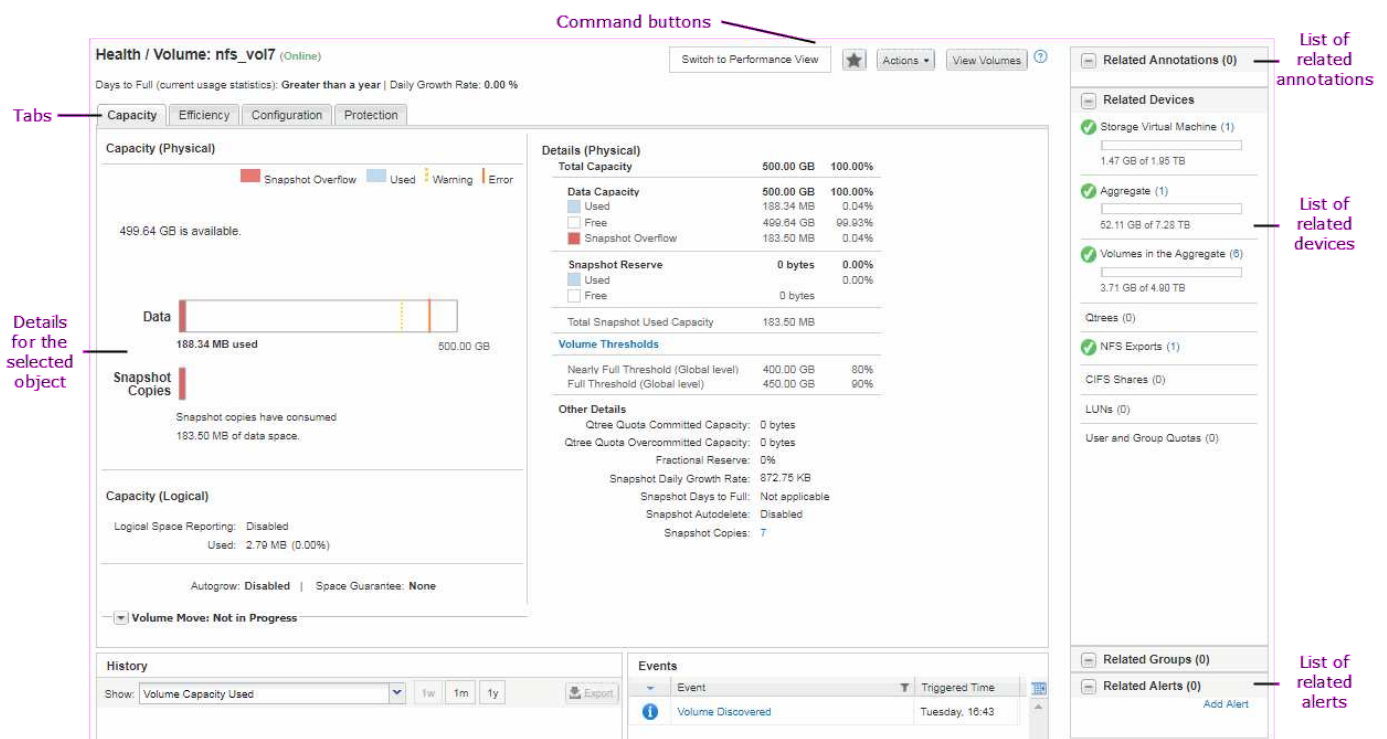
Conoscere i layout tipici delle finestre aiuta a navigare e utilizzare Active IQ Unified Manager in modo efficace. La maggior parte delle finestre di Unified Manager sono simili a uno dei due layout generali: elenco oggetti o dettagli. L'impostazione di visualizzazione consigliata è almeno 1280 per 1024 pixel.

Non tutte le finestre contengono tutti gli elementi nei diagrammi seguenti.

Layout della finestra dell'elenco degli oggetti



Layout della finestra dei dettagli dell'oggetto



Personalizzazione del layout della finestra

Active IQ Unified Manager consente di personalizzare il layout delle informazioni nelle pagine degli oggetti di rete e di archiviazione. Personalizzando le finestre, è possibile controllare quali dati sono visualizzabili e come vengono visualizzati.

• 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, vengono visualizzate le frecce di ordinamento (▲ E ▼) appaiono per quella colonna.

- **Filtro**

Puoi cliccare sull'icona del filtro () per applicare filtri per personalizzare la visualizzazione delle informazioni nelle pagine degli oggetti di rete e di archiviazione, in modo che vengano visualizzate solo le voci che corrispondono alle condizioni fornite. È possibile applicare i filtri dal riquadro Filtri.

Il riquadro Filtri consente di filtrare la maggior parte delle colonne in base alle opzioni selezionate. Ad esempio, nella vista Integrità: Tutti i volumi, è possibile utilizzare il riquadro Filtri per visualizzare tutti i volumi offline selezionando l'opzione di filtro appropriata in Stato.

Le colonne relative alla capacità in qualsiasi elenco visualizzano sempre i dati sulla capacità nelle unità appropriate, arrotondati a due cifre decimali. Ciò vale anche quando si filtrano le colonne di capacità. Ad esempio, se si utilizza il filtro nella colonna Capacità dati totale nella vista Integrità: 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. Allo stesso modo, 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 % dati disponibili nella vista Salute: Tutti gli aggregati per filtrare i dati superiori al 20,45%, la capacità effettiva del 20,454% viene visualizzata come 20,45%. Allo stesso modo, se si filtrano i 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 che si desidera visualizzare. Dopo aver selezionato le colonne appropriate, puoi riordinarle trascinandole con il mouse.

- **Ricerca**

È possibile utilizzare la casella di ricerca per cercare determinati attributi degli oggetti e perfezionare l'elenco degli articoli nella pagina dell'inventario. Ad esempio, puoi immettere "cloud" per restringere l'elenco dei volumi nella pagina dell'inventario dei volumi e visualizzare tutti i volumi che contengono la parola "cloud".

- **Esportazione dati**

È possibile fare clic sul pulsante **Report** (o sul pulsante **Esporta** per esportare i dati in un formato con valori separati da virgole) (.csv) file, (.pdf) documento o Microsoft Excel (.xlsx) file e utilizzare i dati esportati per creare report.

Utilizzare la Guida di Unified Manager

La Guida include informazioni su tutte le funzionalità incluse in Active IQ Unified Manager. Per trovare informazioni sulle funzionalità e su come utilizzarle, è possibile utilizzare il sommario, l'indice o lo strumento di ricerca.

La guida è disponibile da ogni scheda e dalla barra dei menu dell'interfaccia utente di Unified Manager.

Lo strumento di ricerca nella Guida non funziona per le parole parziali.

- Per saperne di più su campi o parametri specifici, fare clic su  .
- Per visualizzare tutti i contenuti della Guida, fare clic su  * > ***Aiuto/Documentazione** nella barra dei menu.

Per informazioni più dettagliate, espandere una qualsiasi parte dell'indice 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.

Aggiungi ai preferiti i tuoi argomenti della Guida preferiti

Nella scheda Preferiti della Guida puoi aggiungere ai preferiti gli argomenti della Guida che utilizzi più frequentemente. I segnalibri della Guida forniscono un accesso rapido ai tuoi argomenti preferiti.

Passi

1. Vai all'argomento della Guida che vuoi aggiungere ai preferiti.
2. Fare clic su **Preferiti**, quindi su **Aggiungi**.

Cerca oggetti di archiviazione

Per accedere rapidamente a un oggetto specifico, puoi utilizzare il campo **Cerca tutti gli oggetti di archiviazione** nella parte superiore della barra dei menu. Questo metodo di ricerca globale su tutti gli oggetti consente di individuare rapidamente oggetti specifici in base al tipo. I risultati della ricerca vengono ordinati in base al tipo di oggetto di archiviazione ed è possibile filtrarli ulteriormente per oggetto utilizzando il menu a discesa.

Prima di iniziare

- Per eseguire questa attività è necessario disporre di uno dei seguenti ruoli: Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Una ricerca valida deve contenere almeno tre caratteri.

Utilizzando il valore del menu a discesa "Tutti", 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 restringere 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 puoi cercare includono:

- Cluster
- Nodi
- VM di archiviazione
- Aggregati
- Volumi
- Qtrees

- Azioni SMB
- Azioni NFS
- Quote utente o gruppo
- LUN
- Spazi dei nomi NVMe
- Gruppi iniziatori
- Iniziatori
- Gruppo di coerenza

Immettendo un nome di carico di lavoro viene restituito l'elenco dei carichi di lavoro nella categoria Volumi o LUN appropriata.

È possibile fare clic su qualsiasi oggetto nei risultati della ricerca per passare alla pagina dei dettagli sulla salute per quell'oggetto. Se non è presente una pagina di stato diretta per un oggetto, viene visualizzata la pagina Stato dell'oggetto padre. Ad esempio, quando si cerca una LUN specifica, viene visualizzata la pagina dei dettagli SVM in cui risiede la LUN.

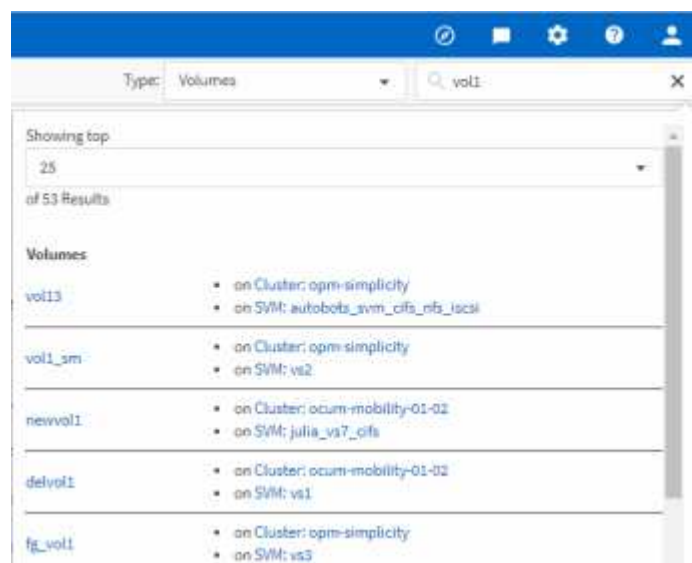


Le porte e i LIF non sono ricercabili nella barra di ricerca globale.

Passi

1. Seleziona un tipo di oggetto dal menu per restringere i risultati della ricerca per un solo tipo di oggetto.
2. Digitare almeno tre caratteri del nome dell'oggetto nel campo **Cerca tutti gli oggetti di archiviazione**.

In questo esempio, nella casella a discesa è selezionato il tipo di oggetto Volumi. Digitando "vol1" nel campo **Cerca tutti gli oggetti di archiviazione** viene visualizzato un elenco di tutti i volumi i cui nomi contengono questi caratteri.



Esportare i dati di archiviazione come report

È possibile esportare i dati di archiviazione in vari formati di output e quindi utilizzare i dati esportati per creare report. Ad esempio, se ci sono 10 eventi critici che non sono stati risolti, puoi esportare i dati dalla pagina dell'inventario di Gestione eventi per creare un

report e quindi inviarlo agli amministratori che possono risolvere i problemi.

È possibile esportare i dati in un .csv file, .xlsx file, o .pdf documento dalle pagine di inventario **Archiviazione e Rete** e utilizzare i dati esportati per creare report. Ci sono altre posizioni nel prodotto in cui solo .csv O .pdf è possibile generare file.

Passi

1. Eseguire una delle seguenti azioni:

Se vuoi esportare...	Fai questo...
Dettagli dell'inventario degli oggetti di archiviazione	Fare clic su Archiviazione o Rete dal menu di navigazione a sinistra, quindi selezionare un oggetto di archiviazione. Scegli una delle viste fornite dal sistema o una vista personalizzata che hai creato.
Dettagli del gruppo di criteri QoS	Fare clic su Archiviazione > Gruppi di criteri QoS dal menu di navigazione a sinistra.
Dettagli sulla capacità di archiviazione e sulla cronologia della protezione	Fare clic su Archiviazione > Aggregati o Archiviazione > Volumi , quindi selezionare un singolo aggregato o volume.
Dettagli dell'evento	Fare clic su Gestione eventi dal menu di navigazione a sinistra.
Dettagli sulle prestazioni dei primi 10 oggetti di archiviazione	Fare clic su Archiviazione > Cluster > Prestazioni:Tutti i cluster , quindi selezionare un cluster e scegliere la scheda Prestazioni migliori . Quindi selezionare un oggetto di archiviazione e un contatore delle prestazioni.

2. Fare clic sul pulsante **Report** (o sul pulsante **Esporta** in alcune pagine dell'interfaccia utente).
3. Fare clic su **Scarica CSV**, **Scarica PDF** o **Scarica Excel** per confermare la richiesta di esportazione.

Dalla scheda Top Performers puoi scegliere di scaricare un report delle statistiche per il singolo cluster che stai visualizzando o per tutti i cluster nel data center.

Il file è stato scaricato.

4. Aprire il file nell'applicazione appropriata.

Informazioni correlate

["Pagina inventario Salute/Cluster"](#)

["Pianificazione di un report"](#)

Filtra il contenuto della pagina dell'inventario

È possibile filtrare i dati della pagina dell'inventario in Unified Manager per individuare rapidamente i dati in base a criteri specifici. È possibile utilizzare i filtri per restringere il contenuto delle pagine di Unified Manager in modo da visualizzare solo i risultati di proprio interesse. Questo fornisce un metodo molto efficiente per visualizzare solo i dati che ti interessano.

Utilizza **Filtro** per personalizzare la visualizzazione della griglia in base alle tue preferenze. Le opzioni di filtro disponibili si basano sul tipo di oggetto visualizzato nella griglia. Se sono attualmente applicati dei filtri, il numero di filtri applicati viene visualizzato a destra del pulsante Filtro.

Sono supportati tre tipi di parametri di filtro.

Parametro	Validazione
Stringa (testo)	Gli operatori sono contiene , inizia con , termina con e non contiene .
Numero	Gli operatori sono maggiore di , minore di , nell'ultimo e tra .
Enum (testo)	Gli operatori sono is e is not .

I campi Colonna, Operatore e Valore sono obbligatori per ciascun filtro; i filtri disponibili riflettono le colonne filtrabili nella pagina corrente. Il numero massimo di filtri che puoi 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 Filtraggio.

1. Nella parte superiore della pagina, fare clic sul pulsante **Filtro**. Viene visualizzato il pannello 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, seleziona o immetti un valore per completare il filtro per quell'oggetto.
5. Per aggiungere un altro filtro, fare clic su **+Aggiungi filtro**. Viene visualizzato un campo filtro aggiuntivo. Completare questo filtro utilizzando la procedura descritta nei passaggi precedenti. Tieni presente che dopo aver aggiunto il quarto filtro, il pulsante **+Aggiungi filtro** non verrà 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 Filtro.
7. Utilizzare il pannello Filtraggio per rimuovere singoli filtri facendo clic sull'icona del cestino a destra del filtro da rimuovere.
8. Per rimuovere tutti i filtri, fare clic su **Reimposta** nella parte inferiore del pannello di filtraggio.

Esempio di filtraggio

L'illustrazione mostra il pannello Filtraggio con tre filtri. Il pulsante **+Aggiungi filtro** viene visualizzato quando si hanno meno del massimo di quattro filtri.

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
+ Add Filter				
				Cancel Apply Filter

Dopo aver cliccato su **Applica filtro**, il pannello Filtraggio si chiude, applica i filtri e mostra il numero di filtri applicati (3).

Visualizza gli eventi attivi dalla campana delle notifiche

La campanella di notifica () nella barra dei menu fornisce un modo rapido per visualizzare gli eventi attivi più importanti monitorati da Unified Manager.

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 include gli eventi informativi. Puoi cliccare su un link per visualizzare l'elenco degli eventi che più ti interessano.

Si noti che quando un cluster non è raggiungibile, Unified Manager visualizza questa informazione in questa pagina. È possibile visualizzare informazioni dettagliate su un cluster non raggiungibile facendo clic sul pulsante **Dettagli**. Questa azione apre la pagina dei dettagli dell'evento. In questa pagina vengono visualizzati anche i problemi di monitoraggio della scala, come spazio insufficiente o RAM insufficiente sulla stazione di gestione.

Passi

1. Dalla barra dei menu, fare clic su .
2. Per visualizzare i dettagli di uno qualsiasi degli eventi attivi, fare clic sul collegamento di testo dell'evento, ad esempio "Capacità 2" o "Prestazioni 4".

Monitora e gestisci i cluster dalla dashboard

La dashboard fornisce informazioni cumulative e immediate sullo stato attuale dei sistemi ONTAP monitorati. La dashboard fornisce dei "pannelli" che consentono di valutare la capacità complessiva, le prestazioni e lo stato di sicurezza dei cluster monitorati.

Inoltre, ci sono alcuni problemi ONTAP che è possibile risolvere direttamente dall'interfaccia utente di Unified Manager, senza dover utilizzare ONTAP System Manager o ONTAP CLI.

Nella parte superiore della dashboard è possibile selezionare se i pannelli devono visualizzare le informazioni per tutti i cluster monitorati o per un singolo cluster. È possibile iniziare visualizzando lo stato di tutti i cluster e poi passare ai singoli cluster quando si desidera visualizzare informazioni dettagliate.



In base alla configurazione, alcuni dei pannelli elencati di seguito potrebbero non essere visualizzati nella pagina.

Pannelli	Descrizione
Azioni di gestione	Quando Unified Manager riesce a diagnosticare e determinare una singola soluzione per un problema, tali soluzioni vengono visualizzate in questo pannello con un pulsante Correggi .
Capacità	Visualizza la capacità totale e utilizzata per il livello locale e il livello cloud, nonché il numero di giorni necessari affinché la capacità locale raggiunga il limite massimo.
Capacità di prestazione	Visualizza il valore della capacità prestazionale per ciascun cluster e il numero di giorni necessari affinché la capacità prestazionale raggiunga il limite superiore.
IOPS del carico di lavoro	Visualizza il numero totale di carichi di lavoro attualmente in esecuzione in un determinato intervallo di IOPS.
Prestazioni del carico di lavoro	Visualizza il numero totale di carichi di lavoro conformi e non conformi assegnati a ciascun livello di servizio di prestazione 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 di archiviazione protette dalla relazione SVM-DR, volumi protetti dalla relazione SnapMirror, volumi protetti da Snapshot e cluster protetti da MetroCluster.
Panoramica sull'utilizzo	Visualizza i cluster ordinati in base al numero più elevato di IOPS, alla velocità effettiva più elevata (MBps) o alla capacità fisica più elevata utilizzata.

Pagina del dashboard

La pagina Dashboard contiene dei "pannelli" che mostrano la capacità di alto livello, le prestazioni e lo stato di sicurezza dei cluster che stai monitorando. Questa pagina fornisce anche un pannello Azioni di gestione in cui sono elencate le correzioni che Unified Manager può apportare per risolvere determinati eventi.

La maggior parte dei pannelli mostra anche il numero di eventi attivi in quella categoria e il numero di nuovi eventi aggiunti nelle 24 ore precedenti. Queste informazioni ti aiutano a decidere quali cluster potresti dover analizzare ulteriormente per risolvere gli eventi. Facendo clic sugli eventi vengono visualizzati gli eventi principali e viene fornito un collegamento alla pagina dell'inventario di Gestione eventi filtrata per mostrare gli eventi attivi in quella categoria.

Nella parte superiore della dashboard è possibile selezionare se i pannelli devono 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 poi passare ai 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

Ci sono alcuni problemi che Unified Manager può diagnosticare in modo approfondito e fornire una soluzione univoca. Se disponibili, tali risoluzioni vengono visualizzate in questo pannello con un pulsante **Correggi** o **Correggi tutto**. È possibile risolvere immediatamente questi problemi da Unified Manager anziché dover utilizzare ONTAP System Manager o ONTAP CLI. Per visualizzare tutti i numeri, clicca su Vedi ["Risolvi i problemi ONTAP direttamente da Unified Manager"](#) per maggiori informazioni.

Pannello di capacità

Quando si visualizzano tutti i cluster, questo pannello mostra la capacità fisica utilizzata (dopo aver applicato i risparmi sull'efficienza di archiviazione) e la capacità fisica disponibile (esclusi i potenziali risparmi sull'efficienza di archiviazione) per ciascun cluster, il numero di giorni fino al riempimento previsto dei dischi e il rapporto di riduzione dei dati (senza copie Snapshot) in base alle impostazioni di efficienza di archiviazione ONTAP configurate. Elenca inoltre la capacità utilizzata per tutti i livelli cloud configurati. Facendo clic sul grafico a barre si accede alla pagina dell'inventario degli aggregati per quel cluster. Facendo clic sul testo "Giorni rimanenti" viene visualizzato un messaggio che identifica l'aggregato con il minor numero di giorni di capacità rimanenti; fare clic sul nome dell'aggregato per visualizzare maggiori dettagli.

Quando si visualizza un singolo cluster, questo pannello mostra la capacità fisica utilizzata e la capacità fisica disponibile per gli aggregati di dati ordinati per ogni singolo tipo di disco sul livello locale e per il livello cloud. Facendo clic sul grafico a barre per un tipo di disco si accede alla pagina Inventario volumi per i volumi che utilizzano quel tipo di disco.

Pannello di capacità prestazionale

Quando si visualizzano tutti i cluster, questo pannello mostra il valore della capacità di prestazione per ciascun cluster (calcolato sulla media dell'ora precedente) e il numero di giorni necessari affinché la capacità di prestazione raggiunga il limite superiore (in base al tasso di crescita giornaliero). Facendo clic sul grafico a barre si accede alla pagina dell'inventario dei nodi per quel cluster. Si noti che la pagina Inventario nodi mostra la capacità prestazionale media delle 72 ore precedenti. Facendo clic sul testo "Giorni al completo" viene visualizzato un messaggio che identifica il nodo con il minor numero di giorni di capacità di prestazione rimanenti; fare clic sul nome del nodo per visualizzare maggiori dettagli.

Quando si visualizza un singolo cluster, questo pannello mostra la percentuale di capacità di prestazioni del cluster utilizzata, i valori totali di IOPS e di throughput totale (MB/s), nonché il numero di giorni che si prevede mancherà prima che ciascuna di queste tre metriche raggiunga il proprio limite massimo.

Pannello IOPS del carico di lavoro

Quando si visualizza un singolo cluster, questo pannello mostra il numero totale di carichi di lavoro attualmente in esecuzione in un determinato intervallo di IOPS e indica il numero per ciascun tipo di disco quando si passa il cursore sul grafico.

Pannello Prestazioni del carico di lavoro

Questo pannello mostra il numero totale di carichi di lavoro conformi e non conformi assegnati a ciascuna

policy PSL (Performance Service Level). Visualizza anche il numero di carichi di lavoro 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 accede ai carichi di lavoro conformi e non conformi assegnati a tale policy.

Pannello di sicurezza

Il pannello Sicurezza presenta lo stato di sicurezza di alto livello per tutti i cluster o per un singolo cluster, a seconda della visualizzazione 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 (conteggio dei cluster conformi e non conformi)
- lo stato di sicurezza della VM di archiviazione (conteggio delle VM di archiviazione conformi e non conformi)
- lo stato di crittografia del volume (conteggio dei volumi crittografati o non crittografati)
- lo stato anti-ransomware del volume (conteggio dei volumi con anti-ransomware abilitati o disabilitati)

È possibile fare clic sui grafici a barre dei cluster conformi e non conformi, delle VM di archiviazione, 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 archiviazione e dei volumi.

La conformità si basa sulla ["Guida al rafforzamento della sicurezza NetApp per ONTAP 9"](#). Fare clic sulla freccia a destra nella parte superiore del pannello per visualizzare i dettagli di sicurezza per tutti i cluster nella pagina Sicurezza. Per informazioni, vedere ["Visualizzazione dello stato di sicurezza dettagliato per cluster e VM di archiviazione"](#).

Pannello di protezione dei dati

Questo pannello visualizza il riepilogo della protezione dei dati per un singolo cluster o per tutti i cluster in un data center. Visualizza il numero totale di eventi di protezione dei dati, eventi MetroCluster e il numero di eventi attivi generati nelle ultime 24 ore in ONTAP. Cliccando sul link di ciascuno di questi eventi verrai indirizzato alla pagina dei dettagli dell'evento. È possibile fare clic sul collegamento **Visualizza tutto** per visualizzare tutti gli eventi di protezione attivi nella pagina dell'inventario Gestione eventi. Il pannello visualizza:

- Numero di volumi in un cluster o di tutti i cluster in un data center protetti da copie Snapshot.
- Numero di volumi in un cluster o di tutti i cluster in un data center protetti da relazioni SnapMirror. Per le relazioni SnapMirror, viene preso in considerazione il conteggio dei volumi nel cluster di origine.
- Numero di cluster o di tutti i cluster in un data center protetti dalla configurazione MetroCluster su IP o FC.
- Il numero di relazioni di volume con l'obiettivo del punto di ripristino (RPO) SnapMirror è in ritardo in base allo stato di ritardo.

È possibile passare il mouse per visualizzare i rispettivi conteggi e le relative legende. È possibile fare clic sulla freccia a destra nella parte superiore del pannello per visualizzare i dettagli di un singolo cluster o di tutti i cluster nella pagina Protezione dati. Puoi anche cliccare:

- I grafici a barre per i volumi non protetti e i volumi protetti da copie Snapshot consentono di accedere alla pagina Volumi e visualizzare i dettagli.
- I grafici a barre per i cluster protetti o non protetti dalla configurazione MetroCluster consentono di accedere alla pagina Cluster e visualizzarne i dettagli.

- I grafici a barre per tutte le relazioni portano alla pagina Relazioni, dove i dettagli vengono filtrati in base al cluster di origine.

Per maggiori informazioni, vedere ["Visualizzazione dello stato di protezione del volume"](#).

Pannello Panoramica sull'utilizzo

Quando si visualizzano tutti i cluster, è possibile scegliere di visualizzarli ordinati in base al numero più elevato di IOPS, alla velocità effettiva più elevata (MB/s) o alla capacità fisica più elevata utilizzata.

Quando si visualizza un singolo cluster, è possibile scegliere di visualizzare i carichi di lavoro ordinati in base al numero più elevato di IOPS, alla velocità effettiva più elevata (MB/s) o alla capacità logica più elevata utilizzata.

Informazioni correlate

["Risoluzione dei problemi tramite le correzioni automatiche di Unified Manager"](#)

["Visualizzazione delle informazioni sugli eventi di performance"](#)

["Gestione delle prestazioni utilizzando la capacità delle prestazioni e le informazioni IOPS disponibili"](#)

["Pagina dei dettagli del volume/salute"](#)

["Analisi e notifica degli eventi prestazionali"](#)

["Descrizione dei tipi di gravità degli eventi"](#)

["Fonti degli eventi di performance"](#)

["Gestire gli obiettivi di sicurezza del cluster"](#)

["Monitora le prestazioni del cluster dalla pagina di destinazione del cluster delle prestazioni"](#)

["Monitorare le prestazioni utilizzando le pagine Inventario delle prestazioni"](#)

Gestisci i problemi o le funzionalità ONTAP direttamente da Unified Manager

È possibile risolvere determinati problemi ONTAP o gestire determinate funzionalità ONTAP direttamente dall'interfaccia utente di Unified Manager, anziché dover utilizzare ONTAP System Manager o ONTAP CLI. L'opzione "Azioni di gestione" fornisce correzioni a una serie di problemi ONTAP che hanno attivato eventi 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 nella Dashboard, nella pagina Dettagli evento e nella selezione Analisi del carico di lavoro nel menu di navigazione a sinistra.

Ci sono alcuni problemi che Unified Manager può diagnosticare in modo approfondito e fornire una soluzione univoca. Per alcune funzionalità ONTAP, come il monitoraggio anti-ransomware, Unified Manager esegue controlli interni e consiglia azioni specifiche. Se disponibili, tali risoluzioni vengono visualizzate in Azioni di gestione con un pulsante **Correggi**. Fare clic sul pulsante **Risolvi** per risolvere il problema. È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Unified Manager invia comandi ONTAP al cluster per apportare 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 archiviazione utilizzando il pulsante **Correggi tutto**. Ad esempio, potrebbero esserci 5 volumi con l'evento "Spazio volume pieno" che potrebbe essere risolto facendo clic sull'azione di gestione **Correggi tutto** per "Abilita aumento automatico volume". Con un clic è possibile risolvere il problema su 5 volumi.

Per informazioni sui problemi e sulle funzionalità ONTAP che è possibile gestire utilizzando la correzione automatica, vedere ["Quali problemi può risolvere Unified Manager"](#).

Quali opzioni ho quando vedo il pulsante Correggi o Correggi tutto?

La pagina Azioni di gestione fornisce il pulsante **Correggi** o **Correggi tutto** per risolvere i problemi di cui Unified Manager è stato informato tramite un evento.

Ti consigliamo di cliccare sui pulsanti per risolvere un problema, se necessario. Tuttavia, se non sei sicuro di voler risolvere il problema come consigliato da Unified Manager, puoi eseguire le seguenti azioni:

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 nascondi questa azione di gestione finché l'evento non verrà generato nuovamente.	Fare clic sulla freccia rivolta verso il basso e quindi su Ignora tutto .
Risolvi 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 Correggi . Quindi seguire i passaggi per correggere o ignorare le singole azioni di gestione.

Cosa vuoi fare?	Azione
Chiedi a Unified Manager di risolvere il problema.	Fare clic sul pulsante Correggi .
Non risolvere il problema in questo momento e nascondi questa azione di gestione finché l'evento non verrà generato di nuovo.	Fare clic sulla freccia rivolta verso il basso e quindi su Ignora .

Cosa vuoi fare?	Azione
Visualizza i dettagli di questo evento per comprendere meglio il problema.	- Fare clic sul pulsante Correggi e verificare la correzione che verrà applicata nella finestra di dialogo visualizzata. - Fare clic sulla freccia rivolta verso il basso e quindi su Visualizza dettagli evento per visualizzare la pagina dei dettagli dell'evento. Quindi fai clic su Correggi da una delle pagine risultanti se vuoi risolvere il problema.
Visualizza i dettagli di questo oggetto di archiviazione per comprendere meglio il problema.	Fare clic sul nome dell'oggetto di archiviazione per visualizzarne i dettagli nella pagina Performance Explorer o Health Details.

In alcuni casi la correzione viene riflessa nel successivo sondaggio di configurazione di 15 minuti. In altri casi potrebbero volerci diverse ore prima che la modifica alla configurazione venga verificata e l'evento diventi obsoleto.

Per visualizzare l'elenco delle azioni di gestione completate o in corso, fare clic sull'icona del filtro e selezionare **Completate** o **In corso**.

Correzione Tutte le operazioni vengono eseguite in serie, quindi quando visualizzi il pannello **In corso** alcuni oggetti avranno lo stato **In corso** mentre altri avranno lo stato **Pianificato**; ciò significa che sono ancora in attesa di essere implementati.

Visualizza lo stato delle azioni di gestione che hai scelto di correggere

Puoi visualizzare lo stato di tutte le azioni di gestione che hai scelto di correggere nella pagina Azioni di gestione. La maggior parte delle azioni vengono visualizzate come **Completate** abbastanza rapidamente dopo che Unified Manager invia il comando ONTAP al cluster. Tuttavia, alcune azioni, come lo spostamento di un volume, potrebbero richiedere più tempo.

Nella pagina Azioni di gestione sono disponibili tre filtri:

- **Completato** mostra sia le azioni di gestione completate con successo sia quelle fallite. Le azioni **non riuscite** forniscono una spiegazione del fallimento, in modo da poter risolvere il problema manualmente.
- **In corso** mostra sia le azioni di gestione in fase di implementazione, sia quelle la cui implementazione è prevista.
- **Consigliato** mostra tutte le azioni di gestione attualmente attive per tutti i cluster monitorati.

Passi

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** nella **Dashboard** e seleziona la vista che desideri visualizzare.

Viene visualizzata la pagina Azioni di gestione.

2. È possibile fare clic sull'icona del cursore accanto all'azione di gestione nel campo **Descrizione** per visualizzare i dettagli sul problema e il comando utilizzato per risolverlo.
3. Per visualizzare le azioni **fallite**, ordinarle in base alla colonna **Stato** nella vista **Completate**. Per lo stesso scopo è possibile utilizzare lo strumento **Filtro**.
4. Se desideri visualizzare maggiori informazioni su un'azione di gestione non riuscita o se decidi di correggere un'azione di gestione consigliata, puoi fare clic su **Visualizza dettagli evento** nell'area espansa dopo aver fatto clic sull'icona del cursore accanto all'azione di gestione. Da quella pagina è disponibile il pulsante **Risolvi**.

Quali problemi può risolvere Unified Manager

Utilizzando la funzionalità di correzione automatica di Active IQ Unified Manager, puoi scegliere di risolvere determinati problemi ONTAP o gestire determinate funzionalità ONTAP, come il monitoraggio anti-ransomware, in modo efficace tramite Unified Manager.

Questa tabella descrive i problemi o le funzionalità ONTAP che è possibile gestire direttamente tramite il pulsante **Correggi** o **Correggi tutto** nell'interfaccia utente Web di Unified Manager.

Nome e descrizione dell'evento	Azione di gestione	Operazione "Riparalo"
Spazio del volume pieno Il volume è quasi esaurito e ha superato la soglia di capacità massima. Questa soglia è impostata di default sul 90% della dimensione del volume.	Abilita l'aumento automatico del volume	Unified Manager determina che l'aumento automatico del volume non è configurato per questo volume, quindi abilita questa funzionalità affinché la capacità del volume aumenti quando necessario.
Inode completi Questo volume ha esaurito gli inode e non può accettare nuovi file.	Aumenta il numero di inode sul volume	Aumenta del 2 per cento il numero di inode sul volume.
Rilevata mancata corrispondenza dei criteri di livello di archiviazione Il volume contiene molti dati inattivi e l'attuale criterio di suddivisione in livelli è impostato su "solo snapshot" o "nessuno".	Abilita la suddivisione automatica in livelli del cloud	Poiché il volume risiede già su un FabricPool, modifica la politica di suddivisione in livelli in "auto", in modo che i dati inattivi vengano spostati nel livello cloud più economico.
Rilevata mancata corrispondenza del livello di archiviazione Il volume contiene molti dati inattivi, ma non risiede su un livello di archiviazione abilitato al cloud (FabricPool).	Modifica il livello di archiviazione dei volumi	Sposta il volume nel livello di archiviazione abilitato al cloud e imposta il criterio di suddivisione in livelli su "automatico" per spostare i dati inattivi nel livello cloud.

Nome e descrizione dell'evento	Azione di gestione	Operazione "Riparalo"
Registro di controllo disabilitato Il registro di controllo non è abilitato per la VM di archiviazione	Abilita la registrazione di controllo per la VM di archiviazione	Abilita la registrazione degli audit sulla VM di archiviazione. Si noti che la VM di archiviazione deve già disporre di una posizione di registro di controllo locale o remota configurata.
Banner di accesso disabilitato Il banner di accesso per il cluster dovrebbe essere abilitato per aumentare la sicurezza rendendo chiare le restrizioni di accesso.	Imposta il banner di accesso per il cluster	Imposta il banner di accesso al cluster su "Accesso limitato agli utenti autorizzati".
Banner di accesso disabilitato Il banner di accesso per la VM di archiviazione dovrebbe essere abilitato per aumentare la sicurezza rendendo chiare le restrizioni di accesso.	Imposta il banner di accesso per la VM di archiviazione	Imposta il banner di accesso alla VM di archiviazione su "Accesso limitato agli utenti autorizzati".
SSH utilizza cifrari non sicuri I cifrari con il suffisso "-cbc" sono considerati non sicuri.	Rimuovere i cifrari non sicuri dal cluster	Rimuove i cifrari non sicuri, come aes192-cbc e aes128-cbc, dal cluster.
SSH utilizza cifrari non sicuri I cifrari con il suffisso "-cbc" sono considerati non sicuri.	Rimuovere i cifrari non sicuri dalla VM di archiviazione	Rimuove i cifrari non sicuri, come aes192-cbc e aes128-cbc, dalla VM di archiviazione.
AutoSupport HTTPS AutoSupport disabilitato Il protocollo di trasporto utilizzato per inviare messaggi AutoSupport al supporto tecnico deve essere crittografato.	Imposta HTTPS come protocollo di trasporto per i messaggi AutoSupport	Imposta HTTPS come protocollo di trasporto per i messaggi AutoSupport sul cluster.

Nome e descrizione dell'evento	Azione di gestione	Operazione "Riparalo"
Soglia di squilibrio del carico del cluster violata Indica che il carico è sbilanciato tra i nodi del cluster. Questo evento viene generato quando la varianza della capacità di prestazione utilizzata è superiore al 30% tra i nodi.	Bilanciare i 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.
Superata la soglia di squilibrio della capacità del cluster Indica che la capacità è sbilanciata tra gli aggregati nel cluster. Questo evento si genera quando la varianza della capacità utilizzata è superiore al 70% tra gli aggregati.	Capacità del cluster di bilanciamento	Unified Manager identifica il volume migliore da spostare da un aggregato all'altro per ridurre lo squilibrio e quindi sposta il volume.
Superamento della soglia di capacità di prestazione utilizzata Indica che il carico sul nodo potrebbe diventare sovrautilizzato se non si riduce l'utilizzo da parte di uno o più carichi di lavoro altamente attivi. Questo evento viene generato quando il valore della capacità di prestazioni utilizzata del nodo è superiore al 100% per più di 12 ore.	Limita il carico elevato sul nodo	Unified Manager identifica il volume con gli IOPS più elevati e applica una policy QoS utilizzando i livelli storici previsti e di picco degli IOPS per ridurre il carico sul nodo.
Soglia di avviso evento dinamico violata Indica che il nodo sta già operando in uno stato di sovraccarico a causa del carico anormalmente elevato di alcuni carichi di lavoro.	Ridurre il sovraccarico nel nodo	Unified Manager identifica il volume con gli IOPS più elevati e applica una policy QoS utilizzando i livelli storici previsti e di picco degli IOPS per ridurre il carico sul nodo.
L'acquisizione non è possibile Al momento il failover è disabilitato, quindi l'accesso alle risorse del nodo durante un'interruzione o un riavvio andrebbe perso finché il nodo non tornasse disponibile.	Abilita il failover del nodo	Unified Manager invia il comando appropriato per abilitare il failover su tutti i nodi del cluster.

Nome e descrizione dell'evento	Azione di gestione	Operazione "Riparalo"
L'opzione Cf.takeover.on_panic è configurata su OFF L'opzione nodeshell "cf.takeover.on_panic" è impostata su off, il che potrebbe causare un problema nei sistemi configurati HA.	Abilita l'acquisizione in caso di panico	Unified Manager invia il comando appropriato al cluster per modificare questa impostazione su on .
Disabilita l'opzione snapmirror.enable di nodeshell La vecchia opzione nodeshell "snapmirror.enable" è impostata su on, il che potrebbe causare un problema durante l'avvio dopo l'aggiornamento a ONTAP 9.3 o versione successiva.	Imposta l'opzione snapmirror.enable su off	Unified Manager invia il comando appropriato al cluster per modificare questa impostazione su off .
Telnet abilitato Indica un potenziale problema di sicurezza perché Telnet non è sicuro e trasmette i dati in modo non crittografato.	Disabilita Telnet	Unified Manager invia il comando appropriato al cluster per disabilitare Telnet.
Configurare l'apprendimento anti-ransomware della VM di archiviazione Controlla periodicamente la presenza di cluster con licenze per il monitoraggio anti-ransomware. Verifica se una VM di archiviazione supporta solo volumi NFS o SMB in tale cluster.	Metti le VM di archiviazione in un <code>learning</code> modalità di monitoraggio anti-ransomware	Unified Manager imposta il monitoraggio anti-ransomware su <code>learning</code> stato per le VM di archiviazione tramite la console di gestione del cluster. Il monitoraggio anti-ransomware su tutti i nuovi volumi creati sulla VM di archiviazione viene automaticamente spostato in 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.

Nome e descrizione dell'evento	Azione di gestione	Operazione "Riparalo"
Configurare l'apprendimento anti-ransomware del volume Controlla periodicamente la presenza di cluster con licenze per il monitoraggio anti-ransomware. Verifica se un volume supporta solo i servizi NFS o SMB in tale cluster.	Metti i volumi in <code>learning</code> modalità di monitoraggio anti-ransomware	Unified Manager imposta il monitoraggio anti-ransomware su <code>learning</code> 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.
Abilita l'anti-ransomware del volume Controlla periodicamente la presenza di cluster con licenze per il monitoraggio anti-ransomware. Rileva se i volumi sono in <code>learning</code> modalità di monitoraggio anti-ransomware per più di 45 giorni e determina la possibilità di metterli in modalità attiva.	Metti i volumi in <code>active</code> modalità di monitoraggio anti-ransomware	Unified Manager imposta il monitoraggio anti-ransomware su <code>active</code> sui 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, nonché creare avvisi per azioni di protezione dei dati.
Disabilita l'anti-ransomware del volume Controlla 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).	Disabilita il monitoraggio anti-ransomware sui volumi	Unified Manager disabilita il monitoraggio anti-ransomware sui volumi tramite la console di gestione del cluster.

Sovrascrivere le azioni di gestione tramite script

È possibile creare script personalizzati e associarli ad avvisi per intraprendere azioni specifiche per eventi specifici, senza optare per le azioni di gestione predefinite disponibili nella pagina Azioni di gestione o nella dashboard di Unified Manager.

Se si desidera intraprendere azioni specifiche per un tipo di evento e si sceglie di non correggerle come parte della capacità 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 Azioni di gestione o nella dashboard di Unified Manager.

Gestire i cluster

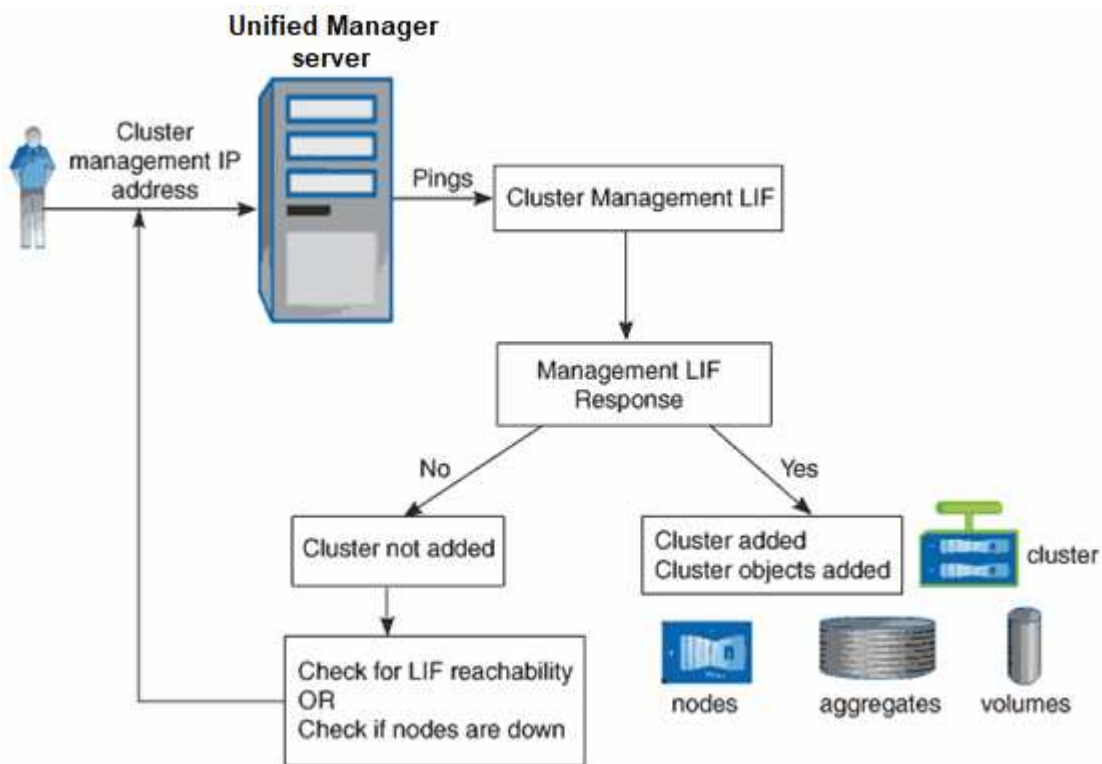
È possibile gestire i cluster ONTAP utilizzando Unified Manager per monitorare, aggiungere, modificare e rimuovere i cluster.

Come funziona il processo di scoperta del cluster

Dopo aver aggiunto un cluster a Unified Manager, il server rileva gli oggetti del cluster e li aggiunge al proprio database. Comprendere il funzionamento del processo di individuazione ti aiuta a gestire i cluster della tua organizzazione e i relativi oggetti.

L'intervallo di monitoraggio per la raccolta delle informazioni sulla configurazione del cluster è di 15 minuti. Ad esempio, dopo aver aggiunto un cluster, occorrono 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 verranno visualizzati nell'interfaccia utente dopo il successivo intervallo di polling, che potrebbe durare fino a 15 minuti.

L'immagine seguente illustra il processo di scoperta:



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



Poiché la raccolta di 15 giorni di dati sulle prestazioni richiede un uso intensivo della CPU, si consiglia di scaglionare l'aggiunta di nuovi cluster in modo che i sondaggi sulla raccolta della continuità dei dati non vengano eseguiti su troppi cluster contemporaneamente.

Visualizza l'elenco dei cluster monitorati

È possibile utilizzare la pagina Configurazione cluster per visualizzare l'inventario dei cluster. È possibile visualizzare i dettagli sui cluster, come il nome o l'indirizzo IP e lo stato della comunicazione.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Fare un passo

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.

Vengono visualizzati tutti i cluster nell'ambiente di archiviazione gestiti da Unified Manager. L'elenco dei cluster è ordinato in base alla colonna del livello di gravità dello stato della raccolta. È possibile fare clic sull'intestazione di una colonna per ordinare i cluster in base a colonne diverse.

Aggiungi cluster

È possibile aggiungere un cluster ad Active IQ Unified Manager in modo da poterlo monitorare. Ciò include la possibilità di ottenere informazioni sul cluster, quali integrità, capacità, prestazioni e configurazione del cluster, in modo da poter individuare e risolvere eventuali problemi che potrebbero verificarsi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o di Amministratore dell'archiviazione.
- È necessario disporre delle seguenti informazioni:
 - Unified Manager supporta cluster ONTAP on-premise, ONTAP Select Cloud Volumes ONTAP.
 - 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, è necessario risolverlo nell'indirizzo IP di gestione del cluster per il LIF di gestione del cluster. Se si utilizza un LIF di gestione dei nodi, l'operazione fallisce.

- Per accedere al cluster è necessario disporre del nome utente e della password.

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

- È necessario conoscere il numero di porta per connettersi al cluster tramite il protocollo HTTPS (in genere la porta 443).
- Il cluster deve eseguire il software ONTAP versione 9.9 o successiva.
- È necessario disporre di spazio adeguato sul server Unified Manager. Non è possibile aggiungere un cluster al server quando è già stato utilizzato più del 90% dello spazio.

- Hai i certificati richiesti:

Certificato SSL (HTTPS): Questo certificato è di proprietà di Unified Manager. Con una nuova installazione di Unified Manager viene generato un certificato SSL autofirmato predefinito (HTTPS). NetApp consiglia di aggiornarlo al certificato firmato da una 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 sicurezza HTTPS"](#).

Certificato EMS: Questo certificato è di proprietà di Unified Manager. Viene utilizzato durante l'autenticazione per le notifiche EMS ricevute da ONTAP.

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 ONTAP. Se il cluster che esegue la versione ONTAP è precedente alla 9.5, l'autenticazione basata su certificato non è abilitata.

L'autenticazione basata su certificato non viene abilitata automaticamente per un cluster se si aggiorna una versione precedente di Unified Manager. Tuttavia, è possibile abilitarlo 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"](#).



- È possibile aggiungere un cluster dall'interfaccia utente Web e l'autenticazione basata su certificato verrà abilitata automaticamente.
- È possibile aggiungere un cluster tramite Unified Manager CLI; l'autenticazione basata su certificato non è abilitata per impostazione predefinita. Se si aggiunge un cluster tramite Unified Manager CLI, è necessario modificare il cluster tramite l'interfaccia utente di Unified Manager. Puoi vedere ["Comandi CLI di Unified Manager supportati"](#) per aggiungere un cluster utilizzando Unified Manager CLI.
- Se per un cluster è abilitata l'autenticazione basata su certificato e si esegue il backup di Unified Manager da un server e lo si ripristina su un altro server Unified Manager in cui il nome host o l'indirizzo IP è stato modificato, il monitoraggio del cluster potrebbe non riuscire. Per evitare il fallimento, modificare e salvare i dettagli del cluster. Per ulteriori informazioni sulla modifica dei dettagli del cluster, vedere ["Modifica dei cluster"](#).
- A livello di cluster, l'interfaccia Active IQ aggiunge due nuove voci di gruppo utenti per il metodo di autenticazione "cert".

+

Certificati cluster: Questo certificato è di proprietà di ONTAP. Non è possibile aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato è già scaduto, è necessario rigenerarlo prima di aggiungere il cluster. Per informazioni sulla generazione del certificato, 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 supportati, è necessario installare un'istanza aggiuntiva di Unified Manager per monitorare alcuni cluster. Per visualizzare l'elenco dei conteggi dei nodi supportati, vedere ["Guida alle migliori pratiche di Unified Manager"](#).

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.

2. Nella pagina Configurazione cluster, fare clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi cluster, specificare i valori richiesti, quindi fare clic su **Invia**.
4. Nella finestra di dialogo Autorizza host, fare clic su **Visualizza certificato** per visualizzare le informazioni sul certificato del cluster.
5. Fare clic su **Sì**.

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.

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



- La raccolta di dati sulle prestazioni per 15 giorni richiede un uso intensivo della CPU. NetApp consiglia di scaglionare l'aggiunta di nuovi cluster in modo che i poll di raccolta della continuità dei dati non vengano eseguiti contemporaneamente su troppi cluster. Inoltre, se si riavvia Unified Manager durante il periodo di raccolta della continuità dei dati, la raccolta viene interrotta e si noteranno delle lacune nei grafici delle prestazioni per il periodo di tempo mancante.
- Quando si aggiunge un cluster ONTAP con versione 9.14.1 o successiva, la comunicazione avviene tramite la funzionalità agente cloud. ONTAP crea automaticamente un utente con account di servizio interno con privilegi di sola lettura (ad esempio, clus-agent-xxxx). Unified Manager interrompe la raccolta dei dati da tali cluster se clus-agent l'utente è stato eliminato.

Se ricevi un messaggio di errore che indica che non è possibile aggiungere il cluster, verifica se si verificano i seguenti problemi:



- Se gli orologi sui 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 tramite NTP o un servizio simile.
- Se il cluster ha raggiunto il numero massimo di destinazioni di notifica EMS, non è possibile aggiungere l'indirizzo Unified Manager. Per impostazione predefinita, è possibile definire solo 20 destinazioni di notifica EMS sul cluster.

Informazioni correlate

["Aggiunta di utenti"](#)

["Visualizzazione dell'elenco e dei dettagli dei cluster"](#)

["Installazione di un certificato HTTPS firmato e restituito da una CA"](#)

Modifica 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 **Modifica cluster**.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o di Amministratore dell'archiviazione.



A partire da Unified Manager 9.7, i cluster possono essere aggiunti solo tramite HTTPS.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.
2. Nella pagina **Configurazione cluster**, seleziona il cluster che desideri modificare, quindi fai clic su **Modifica**.
3. Nella finestra di dialogo **Modifica cluster**, modificare i valori come desiderato. + Se hai modificato i dettagli di un cluster aggiunto a Unified Manager, puoi visualizzare i dettagli del certificato per la comunicazione Mutual TLS, in base alla versione ONTAP . Per maggiori informazioni sulla versione ONTAP , vedere ["Certificati per la comunicazione TLS reciproca"](#) . + È possibile visualizzare i dettagli del certificato facendo 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 Autorizza host, fare clic su **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 dei cluster"](#)

Rimuovi i cluster

È possibile rimuovere un cluster da Unified Manager utilizzando la pagina Configurazione cluster. Ad esempio, è possibile rimuovere un cluster se il rilevamento del cluster non riesce o quando si desidera dismettere un sistema di archiviazione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o di Amministratore dell'archiviazione.

Questa attività rimuove il cluster selezionato da Unified Manager. Una volta rimosso, un cluster non viene più monitorato. Anche l'istanza di Unified Manager registrata nel cluster rimosso viene annullata dalla registrazione nel cluster.

La rimozione di un cluster elimina anche tutti i suoi oggetti di archiviazione, i dati storici, i servizi di archiviazione e tutti gli eventi associati da Unified Manager. Tali modifiche vengono riflesse nelle pagine dell'inventario e nelle pagine dei dettagli dopo il successivo ciclo di raccolta dati.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.
2. Nella pagina Configurazione cluster, seleziona il cluster che desideri rimuovere e fai clic su **Rimuovi**.
3. Nella finestra di dialogo del messaggio **Rimuovi origine dati**, fare clic su **Rimuovi** per confermare la richiesta di rimozione.

Informazioni correlate

["Aggiunta di utenti"](#)

["Visualizzazione dell'elenco e dei dettagli dei cluster"](#)

Riscoprire i cluster

È possibile riscoprire manualmente un cluster dalla pagina Configurazione cluster per ottenere le informazioni più recenti sullo stato di integrità, di monitoraggio e sulle prestazioni del cluster.

È possibile riscoprire manualmente un cluster quando si desidera aggiornarlo, ad esempio aumentando le dimensioni di un aggregato quando lo spazio non è sufficiente, e si desidera che Unified Manager rilevi le modifiche apportate.

Quando Unified Manager è associato a OnCommand Workflow Automation (WFA), l'associazione attiva la riacquisizione dei dati memorizzati nella cache da WFA.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.
2. Nella pagina **Configurazione cluster**, fare clic su **Riscopri**.

Unified Manager riscopre il cluster selezionato e visualizza lo stato di integrità e le prestazioni più recenti.

Informazioni correlate

["Visualizzazione dell'elenco e dei dettagli dei cluster"](#)

Monitorare l'infrastruttura virtuale VMware

Active IQ Unified Manager fornisce visibilità sulle macchine virtuali (VM) nella tua infrastruttura virtuale e consente il monitoraggio e la risoluzione dei problemi di archiviazione e prestazioni nel tuo ambiente virtuale. È possibile utilizzare questa funzionalità per determinare eventuali problemi di latenza nell'ambiente di archiviazione o quando viene segnalato un evento di prestazioni sul server vCenter.

Una tipica distribuzione di un'infrastruttura virtuale su ONTAP presenta vari componenti distribuiti tra i livelli di elaborazione, rete e archiviazione. Eventuali ritardi nelle prestazioni di un'applicazione VM potrebbero verificarsi a causa di una combinazione di latenze riscontrate dai vari componenti ai rispettivi livelli. Questa funzionalità è utile per gli amministratori di storage e vCenter Server e per i tecnici IT generalisti che hanno bisogno di analizzare un problema di prestazioni in un ambiente virtuale e capire in quale componente si è verificato il problema.

Ora è possibile accedere a vCenter Server dal menu vCenter della sezione VMware. La vista panoramica di

ciascuna macchina virtuale elencata presenta il collegamento **VCENTER SERVER** nella VISTA TOPOLOGIA che avvia vCenter Server in un nuovo browser. È anche possibile utilizzare il pulsante **Espandi topologia** per avviare vCenter Server e fare clic sul pulsante **Visualizza in vCenter** per visualizzare i datastore in vCenter Server.

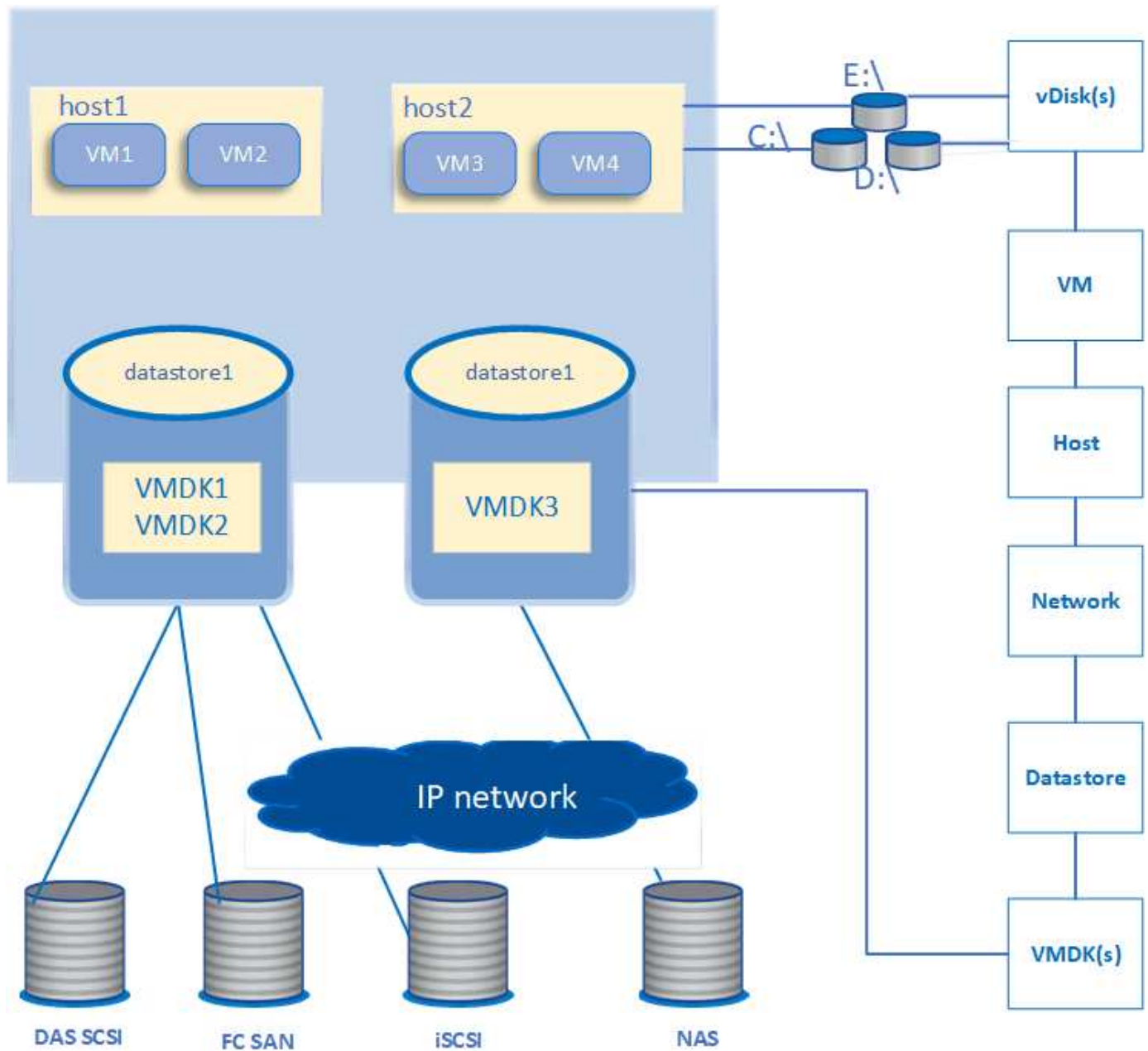
Unified Manager presenta il sottosistema sottostante di un ambiente virtuale in una vista topologica per determinare se si è verificato un problema di latenza nel nodo di elaborazione, nella rete o nell'archiviazione. La vista evidenzia anche l'oggetto specifico che causa il ritardo nelle prestazioni per l'adozione di misure correttive e la risoluzione del problema di fondo.

Un'infrastruttura virtuale distribuita su storage ONTAP include i seguenti oggetti:

- vCenter Server: un piano di controllo centralizzato per la gestione delle VM 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 VM.
- Datastore: i datastore sono oggetti di archiviazione virtuali connessi agli host ESXi. I datastore sono entità di archiviazione gestibili di ONTAP, come LUN o volumi, utilizzati come repository per i file VM, come file di registro, script, file di configurazione e dischi virtuali. Sono collegati agli host nell'ambiente tramite una connessione di rete SAN o IP. Gli archivi dati esterni a ONTAP mappati su vCenter Server non sono supportati né visualizzati su Unified Manager.
- VM: una macchina virtuale VMware.
- Dischi virtuali: i dischi virtuali sui datastore appartenenti alle VM che hanno un'estensione come VMDK. I dati di un disco virtuale vengono archiviati sul VMDK corrispondente.
- VMDK: un disco di macchina virtuale sul datastore che fornisce spazio di archiviazione per i dischi virtuali. Per ogni disco virtuale esiste un VMDK corrispondente.

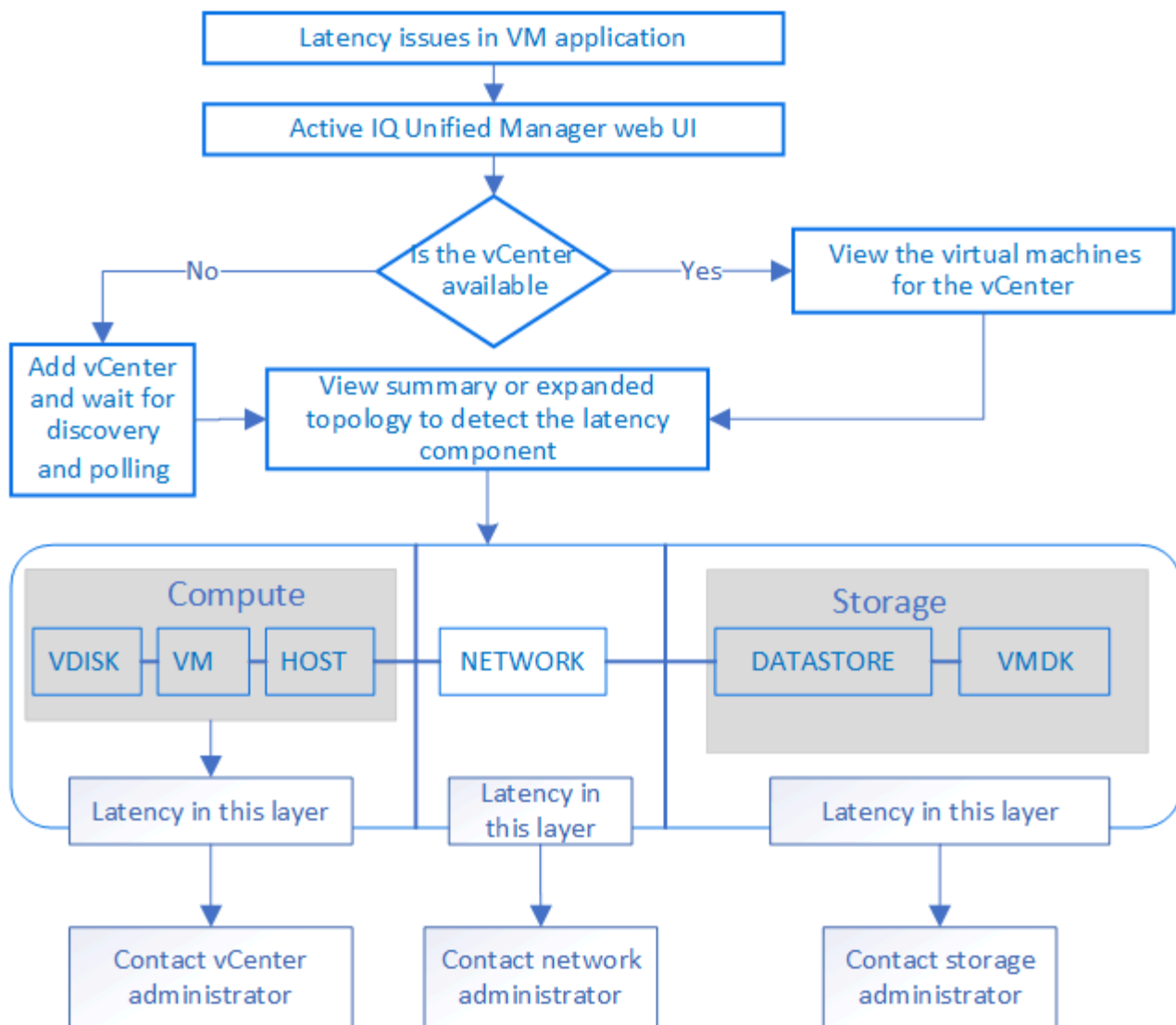
Questi oggetti sono rappresentati in una vista topologica della VM.

Virtualizzazione VMware su ONTAP



Flusso di lavoro dell'utente

Il diagramma seguente mostra un tipico caso d'uso della vista topologia VM:



Cosa non è supportato

- Gli archivi dati esterni a ONTAP e mappati alle istanze di vCenter Server non sono supportati su Unified Manager. Non sono supportate nemmeno le VM con dischi virtuali su tali datastore.
- Non è supportato un datastore che si estende su più LUN.
- Gli archivi dati che utilizzano la traduzione degli indirizzi di rete (NAT) per la mappatura dei dati LIF (endpoint di accesso) non sono supportati.
- L'esportazione di volumi o LUN come datastore su cluster diversi con gli stessi indirizzi IP in una configurazione con più LIF non è supportata poiché Unified Manager non è in grado di identificare quale datastore appartiene a quale cluster.

Esempio: supponiamo che il cluster A abbia il datastore A. Il datastore A viene esportato tramite dati LIF con lo stesso indirizzo IP xxxx e la VM A viene creata su questo datastore. Analogamente, il cluster B ha il datastore B. Il datastore B viene esportato tramite LIF dati con lo stesso indirizzo IP xxxx e la VM B viene creata sul datastore B. UM non sarà in grado di mappare il datastore A per la topologia della VM A sul volume ONTAP /LUN corrispondente né di mappare la VM B.

- Come datastore sono supportati solo i volumi NAS e SAN (iSCSI e FCP per VMFS), i volumi virtuali (vVols) 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 analizzare le 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 in modo che punti alle LUN attive negli scenari di switchover e switchback. Senza un intervento manuale, i loro archivi dati diventano inaccessibili.

Visualizza e aggiungi 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 .

Prima di iniziare

Prima di aggiungere o visualizzare vCenter Server, verificare quanto segue:

- Conosci i nomi dei vCenter Server.
- Conosci l'indirizzo IP di vCenter Server e disponi delle credenziali richieste. Le credenziali devono essere quelle di un amministratore di vCenter Server o di un utente root con accesso in sola lettura a vCenter Server.
- Il vCenter Server che desideri aggiungere esegue vSphere 6.5 o versioni successive.



Il supporto di Unified Manager per VMware ESXi e vCenter Server è disponibile in lingua inglese e giapponese.

- L'impostazione di raccolta dati in vCenter Server è impostata sul livello statistico di *Level 3* , garantendo il livello richiesto di raccolta delle metriche per tutti gli oggetti monitorati. La durata dell'intervallo dovrebbe essere *5 minutes* e il periodo di salvataggio dovrebbe essere *1 day* .

Per ulteriori informazioni, consultare la sezione “Livelli di raccolta dati” della *Guida al monitoraggio e alle prestazioni di vSphere* nella documentazione VMware.

- Per calcoli corretti dei valori di latenza, i valori di latenza in vCenter Server sono configurati in millisecondi e non in microsecondi.
- Durante l'aggiunta del datastore a vCenter Server, è possibile utilizzare sia l'indirizzo IP dell'host sia il nome di dominio completo (FQDN). Se si aggiunge un 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 nel `/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 riuscito.
- Quando si aggiunge vCenter Server a Unified Manager, si ottiene l'accesso in lettura a VMware SDK. Ciò è necessario per il polling della configurazione.

Per ogni vCenter Server aggiunto e rilevato, Unified Manager raccoglie i dati di configurazione, come i dettagli del vCenter Server e del server ESXi, la mappatura ONTAP , i dettagli del datastore e il numero di VM ospitate. Raccoglie inoltre le metriche delle prestazioni dei componenti.

Passi

1. Vai su **VMWARE > vCenter** e controlla se il tuo vCenter Server è disponibile nell'elenco.



Se il tuo vCenter Server non è disponibile, devi aggiungerlo.

- a. Fare clic su **Aggiungi**.
- b. Aggiungere l'indirizzo IP corretto per vCenter Server e assicurarsi che il dispositivo 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 **Salva**.

Una volta effettuata la rilevazione, verrà visualizzato un certificato del server che dovrai 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 VM associate e la raccolta avviene a intervalli pianificati.

2. Se il tuo vCenter Server è disponibile nella pagina **vCenter**, controllane lo stato passando il mouse sul campo **Stato** per vedere se il tuo vCenter Server funziona come previsto o se c'è un avviso o un errore.



Aggiungendo vCenter Server è possibile visualizzare i seguenti stati. Tuttavia, i dati sulle prestazioni e sulla latenza delle VM corrispondenti potrebbero richiedere fino a un'ora dopo l'aggiunta di vCenter Server per essere riflessi accuratamente.

- Verde: "Normale", indica che vCenter Server è stato rilevato e che le metriche delle prestazioni sono state raccolte correttamente
 - Giallo: "Avviso" (ad esempio, quando il livello di statistiche per vCenter Server non è stato impostato su 3 o superiore per ottenere statistiche per ciascun oggetto)
 - Arancione: "Errore" (indica eventuali errori interni, come eccezioni, errori nella raccolta dei dati di configurazione o vCenter Server non raggiungibile). È possibile fare clic sull'icona di visualizzazione della colonna (**Mostra/Nascondi**) per visualizzare il messaggio di stato per uno 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 > Modifica**.
 4. Apportare le modifiche necessarie nella pagina **Modifica VMware vCenter Server**.
 5. Fare clic su **Salva**.

Inizio della raccolta dati di vCenter Server

vCenter Server raccoglie campioni di dati sulle prestazioni in tempo reale di 20 secondi e li trasforma in campioni di 5 minuti. La pianificazione per la raccolta dei dati sulle prestazioni 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 di IOPS e latenza per i dischi virtuali, le VM e gli host. Per i datastore, 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 prestazioni non sono disponibili immediatamente dopo l'aggiunta di vCenter Server, ma solo all'inizio dell'ora successiva. L'interrogazione dei dati sulle prestazioni inizia al completamento di un ciclo di raccolta dei dati di configurazione.

Per l'interrogazione 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 prestazioni, vedere "Attività di raccolta dei dati sulle prestazioni e sulla configurazione del cluster".

Informazioni correlate

["Attività di raccolta dati sulla configurazione e sulle prestazioni del cluster"](#)

Rimuovere vCenter Server

È possibile rimuovere i server vCenter dall'istanza di Active IQ Unified Manager . Ad esempio, è possibile rimuovere un vCenter Server se il rilevamento di vCenter Server non riesce o quando non è più necessario.

La rimozione di un vCenter Server elimina anche tutte le macchine virtuali (VM) ospitate su quel vCenter e i relativi dati di configurazione. Dopo la rimozione, vCenter Server non verrà più monitorato, né gli oggetti associati né i dati storici. Tali modifiche verranno riflesse nelle pagine di vCenter e dell'inventario delle macchine virtuali.

Prima di iniziare

Prima di rimuovere i server vCenter, verificare quanto segue:

- Hai il ruolo di Amministratore dell'applicazione o di Amministratore dell'archiviazione.
- È necessario conoscere i nomi dei vCenter Server e i rispettivi indirizzi IP ad essi associati.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **VMWARE>vCenter**.
2. Nella pagina vCenter, seleziona il vCenter Server che desideri rimuovere e fai clic su **Rimuovi**.
3. Nella finestra di dialogo del messaggio **Rimuovi vCenter**, fare clic su **OK** per confermare la richiesta di rimozione.

Monitorare le macchine virtuali

In caso di problemi di latenza nelle applicazioni delle macchine virtuali (VM), potrebbe essere necessario monitorare le VM per analizzarne e risolverne la causa. Le VM sono disponibili quando il loro vCenter Server e i cluster ONTAP che ospitano lo storage delle VM vengono aggiunti a Unified Manager.

I dettagli delle VM sono visibili nella pagina **VMWARE > > Macchine virtuali**. Vengono visualizzate informazioni quali disponibilità, stato, capacità utilizzata e allocata, latenza di rete, IOPS e latenza della VM, del datastore e dell'host. Per una VM che supporta più datastore, la griglia mostra le metriche del datastore con la latenza peggiore, con un'icona asterisco (*) che indica i datastore aggiuntivi. Facendo clic sull'icona vengono visualizzate le metriche del datastore aggiuntivo. Alcune di queste colonne non sono disponibili per l'ordinamento e il filtraggio.



Per visualizzare una VM e i relativi dettagli, è necessario che la scoperta (polling o raccolta di metriche) del cluster ONTAP sia completa. Se il cluster viene rimosso da Unified Manager, la VM non sarà più disponibile dopo il successivo ciclo di individuazione.

Da questa pagina è anche possibile visualizzare la topologia dettagliata di una VM, visualizzando i componenti a cui è correlata la VM, ad esempio l'host, il disco virtuale e il datastore ad essa collegati. La vista topologica mostra i componenti sottostanti nei loro livelli specifici, nel seguente ordine: **Disco virtuale > VM > Host > Rete > Datastore > VMDK**.

È possibile determinare il percorso I/O e le latenze a livello di componente da un punto di vista topologico e identificare se l'archiviazione è la causa del problema di prestazioni. La vista riepilogativa della topologia mostra il percorso I/O ed evidenzia il componente che presenta problemi di IOPS e latenza, consentendoti di decidere i passaggi per la risoluzione dei problemi. È anche possibile avere una vista espansa della topologia che descrive ogni componente separatamente insieme alla latenza di quel componente. È possibile selezionare un componente per determinare il percorso I/O evidenziato attraverso i livelli.

Visualizza la topologia riassuntiva

Per determinare i problemi di prestazioni visualizzando le VM in una topologia riepilogativa:

1. Vai su **VMWARE > Macchine virtuali**.
2. Cerca la tua VM digitandone il nome nella casella di ricerca. Puoi anche filtrare i risultati della ricerca in base a criteri specifici cliccando sul pulsante **Filtra**. Tuttavia, se non riesci a trovare la tua VM, assicurati che il vCenter Server corrispondente sia stato aggiunto e rilevato.



I server vCenter consentono l'uso di caratteri speciali (ad esempio %, &, *, \$, #, @, !, \, /, :, *, ?, ", <, >, |, ;, ') nei nomi delle entità vSphere, ad esempio VM, cluster, datastore, cartella o file. VMware vCenter Server ed ESX/ESXi Server non eseguono l'escape dei caratteri speciali utilizzati nei nomi visualizzati. Tuttavia, quando il nome viene elaborato in Unified Manager, viene visualizzato in modo diverso. Ad esempio, una VM denominata come %\$VC_AIQUM_clone_191124% in vCenter Server viene visualizzato come %25\$VC_AIQUM_clone_191124%25 in Unified Manager. È necessario tenere presente questo problema quando si esegue una query su una VM il cui nome contiene caratteri speciali.

3. Controllare lo stato della VM. Gli stati delle VM vengono recuperati da vCenter Server. Sono disponibili i seguenti stati. Per ulteriori informazioni su questi stati, consultare la documentazione VMware.
 - Normale
 - Avvertimento
 - Attenzione
 - Non monitorato
 - Sconosciuto
4. Fare clic sulla freccia rivolta verso il basso accanto alla VM per visualizzare la vista riepilogativa della topologia dei componenti nei livelli di elaborazione, rete e archiviazione. Il nodo che presenta problemi di latenza è evidenziato. La vista riepilogativa mostra la latenza peggiore dei componenti. Ad esempio, se una VM ha più di un disco virtuale, questa vista mostra il disco virtuale con la latenza peggiore tra tutti i dischi virtuali.
5. Per analizzare la latenza e la produttività del datastore in un determinato periodo di tempo, fare clic sul pulsante **Workload Analyzer** sopra l'icona dell'oggetto datastore. Si accede alla pagina Analisi del carico di lavoro, dove è possibile selezionare un intervallo di tempo e visualizzare i grafici delle prestazioni del datastore. Per ulteriori informazioni sull'analizzatore del carico di lavoro, vedere *Risoluzione dei problemi dei carichi di lavoro tramite l'analizzatore del carico di lavoro*.

Visualizza la topologia espansa

È possibile analizzare in dettaglio ciascun componente separatamente visualizzando la topologia espansa della VM.

Passi

1. Dalla vista riepilogativa della topologia, fare clic su **Espandi topologia**. È possibile visualizzare separatamente la topologia dettagliata di ciascun componente con i numeri di latenza per ciascun oggetto. Se in una categoria sono presenti più nodi, ad esempio più nodi nel datastore o nel VMDK, il nodo con la latenza peggiore viene evidenziato in rosso.
2. Per controllare il percorso IO di un oggetto specifico, fare clic sull'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 visualizzare la mappatura evidenziata sul rispettivo VMDK. In caso di ritardo nelle prestazioni di questi componenti, è possibile raccogliere più dati da ONTAP e risolvere il problema.



Le metriche non vengono segnalate per i VMDK. Nella topologia vengono visualizzati solo i nomi VMDK e non le metriche.

Informazioni correlate

["Risoluzione dei problemi dei carichi di lavoro tramite Workload Analyzer"](#)

Visualizza l'infrastruttura virtuale in una configurazione di disaster recovery

È possibile visualizzare le metriche di configurazione e prestazioni dei datastore ospitati in una configurazione MetroCluster o in una configurazione di disaster recovery (SVM DR) di una macchina virtuale di archiviazione (Storage VM).

In Unified Manager è possibile visualizzare i volumi NAS o LUN in una configurazione MetroCluster collegati come datastore in vCenter Server. Gli archivi dati ospitati in una configurazione MetroCluster sono rappresentati nella stessa vista topologica di un archivio dati in un ambiente standard.

È anche possibile visualizzare i volumi NAS o i LUN in una configurazione di disaster recovery di una VM di storage mappati ai datastore in vCenter Server.

Visualizza i datastore nella configurazione MetroCluster

Prima di visualizzare gli archivi dati in una configurazione MetroCluster, tenere presente i seguenti prerequisiti:

- In caso di switchover e switchback, l'individuazione dei cluster primario e secondario della coppia HA e dei server vCenter dovrebbe essere completa.
- I cluster primario e secondario 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 di documentazione ONTAP 9"](#)

Per visualizzare i datastore, seguire questi passaggi:

1. Nella pagina **VMWARE > Macchine virtuali**, fare clic sulla VM che ospita il datastore. Fare clic sul collegamento **Workload Analyzer** o sull'oggetto datastore. Nello scenario standard, quando il sito primario che ospita il volume o la LUN funziona come previsto, è possibile visualizzare i dettagli del cluster vServer del sito primario.
2. In caso di disastro e di un successivo passaggio al sito secondario, il collegamento al datastore punta alle metriche delle prestazioni del volume o LUN nel cluster secondario. Ciò si riflette dopo il completamento

del ciclo successivo di cluster e della scoperta (acquisizione) del vServer.

3. Dopo un passaggio riuscito, il collegamento del datastore riflette nuovamente le metriche delle prestazioni del volume o della LUN nel cluster primario. Ciò si riflette dopo il completamento del ciclo successivo di cluster e della scoperta del vServer.

Visualizza i datastore nella configurazione di ripristino di emergenza della VM di archiviazione

Prima di visualizzare gli archivi dati in una configurazione di ripristino di emergenza della VM di archiviazione, tenere presente i seguenti prerequisiti:

- In caso di switchover e switchback, l'individuazione dei cluster primario e secondario della coppia HA e dei server vCenter dovrebbe essere completa.
- Sia il cluster di origine che quello di destinazione e i peer delle VM di storage devono essere gestiti da Unified Manager.
- La configurazione richiesta deve essere completata su ONTAP e vCenter Server.
 - Per i datastore NAS (NFS e VMFS), in caso di disastro, i passaggi includono l'attivazione della VM di storage secondaria, la verifica dei LIF e dei percorsi dei dati, la creazione delle connessioni perse su vCenter Server e l'avvio delle VM.

Per tornare al sito primario, i dati tra i volumi devono essere sincronizzati prima che il sito primario inizi a fornire i dati.

- Per i datastore SAN (iSCSI e FC per VMFS), vCenter Server formatta la LUN montata in formato VMFS. In caso di disastro, i passaggi includono l'attivazione della VM di archiviazione secondaria e la verifica dei LIF e dei percorsi dei dati. Se gli IP di destinazione iSCSI sono diversi dai LIF primari, devono essere aggiunti manualmente. I nuovi LUN dovrebbero essere disponibili come dispositivi nell'adattatore iSCSI dell'adattatore di archiviazione dell'host. Successivamente, è necessario creare nuovi datastore VMFS con i nuovi LUN e registrare le vecchie VM con nuovi nomi. Le VM devono essere attive e funzionanti.

In caso di ripristino, i dati tra i volumi dovrebbero essere sincronizzati. I nuovi datastore VMFS devono essere nuovamente creati utilizzando le LUN e le vecchie VM registrate con nuovi nomi.

Per informazioni sulla configurazione, consultare la documentazione di ONTAP e vCenter Server.

["Centro di documentazione ONTAP 9"](#)

Per visualizzare i datastore, seguire questi passaggi:

1. Nella pagina **VMWARE > Macchine virtuali**, fare clic sull'inventario VM che ospita il datastore. Fare clic sul collegamento all'oggetto datastore. Nello scenario standard, è possibile visualizzare i dati sulle prestazioni dei volumi e delle LUN nella VM di archiviazione primaria.
2. In caso di disastro e di un passaggio consecutivo alla VM di archiviazione secondaria, il collegamento al datastore punta alle metriche delle prestazioni del volume o della LUN nella VM di archiviazione secondaria. Ciò si riflette dopo il completamento del ciclo successivo di cluster e della scoperta (acquisizione) del vServer.
3. Dopo un passaggio riuscito, il collegamento del datastore riflette nuovamente le metriche delle prestazioni del volume o della LUN nella VM di archiviazione primaria. Ciò si riflette dopo il completamento del ciclo successivo di cluster e della scoperta del vServer.

Scenari non supportati

- Per una configurazione MetroCluster , tenere presenti le seguenti limitazioni:
 - Cluster solo nel NORMAL E SWITCHOVER gli stati vengono presi in considerazione. Altri stati, come PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK , E NOT_REACHABLE non sono supportati.
 - A meno che non sia abilitato il passaggio automatico (ASO), se il cluster primario si arresta, il cluster secondario non può essere rilevato e la topologia continua a puntare al volume o alla LUN nel cluster primario.
- Per una configurazione di disaster recovery di una VM di archiviazione, tenere presente la seguente limitazione:
 - Non è supportata una configurazione con Site Recovery Manager (SRM) o Storage Replication Adapter (SRA) abilitati per un ambiente di archiviazione SAN.

Fornire e gestire i carichi di lavoro

La funzionalità di gestione attiva di Active IQ Unified Manager fornisce livelli di servizio delle prestazioni, criteri di efficienza dello storage e API del provider di storage per il provisioning, il monitoraggio e la gestione dei carichi di lavoro di storage in un data center.



Unified Manager fornisce questa funzionalità per impostazione predefinita. Se non si prevede di utilizzare questa funzionalità, è possibile disattivarla da **Gestione archiviazione > Impostazioni funzionalità**.

Se abilitata, è possibile eseguire il provisioning dei carichi di lavoro sui cluster ONTAP gestiti dall'istanza di Unified Manager. È inoltre possibile assegnare policy, come i livelli di servizio delle prestazioni e le policy di efficienza dell'archiviazione, ai carichi di lavoro e gestire l'ambiente di archiviazione in base a tali policy.

Questa funzionalità abilita le seguenti funzioni:

- Rilevamento automatico dei carichi di lavoro di archiviazione sui cluster aggiunti, consentendo una facile valutazione e distribuzione dei carichi di lavoro di archiviazione
- Provisioning di carichi di lavoro NAS che supportano i protocolli NFS e CIFS
- Provisioning di carichi di lavoro SAN che supportano i protocolli iSCSI e FCP
- Supporto per i protocolli NFS e CIFS sulla stessa condivisione file
- Gestione dei livelli di servizio delle prestazioni e delle politiche di efficienza dello storage
- Assegnazione di livelli di servizio delle prestazioni e policy di efficienza di archiviazione ai carichi di lavoro di archiviazione

Le opzioni **Provisioning**, **Storage > Workloads** e **Policies** nel riquadro sinistro dell'interfaccia utente consentono di modificare varie configurazioni.

Utilizzando queste opzioni è possibile eseguire le seguenti funzioni:

- Visualizza i carichi di lavoro di archiviazione nella pagina **Archiviazione > Carichi di lavoro**
- Crea carichi di lavoro di archiviazione dalla pagina Provision Workload
- Creare e gestire i livelli di servizio delle prestazioni dalle policy

- Crea e gestisci criteri di efficienza di archiviazione da Criteri
- Assegnare policy ai carichi di lavoro di archiviazione dalla pagina Carichi di lavoro

Informazioni correlate

["Gestione dell'archiviazione basata su policy"](#)

Panoramica dei carichi di lavoro

Un carico di lavoro rappresenta le operazioni di input/output (I/O) di un oggetto di archiviazione, ad esempio un volume o una LUN. Il modo in cui viene fornito lo storage si basa sui requisiti previsti del carico di lavoro. Le statistiche del carico di lavoro vengono monitorate da Active IQ Unified Manager solo dopo che si è verificato traffico da e verso l'oggetto di archiviazione. Ad esempio, i valori IOPS e latenza del carico di lavoro sono disponibili dopo che gli utenti iniziano a utilizzare un database o un'applicazione di posta elettronica.

La pagina Carichi di lavoro visualizza un riepilogo dei carichi di lavoro di archiviazione dei cluster ONTAP gestiti da Unified Manager. Fornisce informazioni cumulative e immediate sui carichi di lavoro di archiviazione conformi al Performance Service Level, nonché sui carichi di lavoro di archiviazione non conformi. Consente inoltre di valutare la capacità e le prestazioni (IOPS) totali, disponibili e utilizzate dei cluster nel data center.



Si consiglia di valutare il numero di carichi di lavoro di archiviazione non conformi, non disponibili o non gestiti da alcun Performance Service Level e di adottare le misure necessarie per garantirne la conformità, l'utilizzo della capacità e gli IOPS.

La pagina Carichi di lavoro è composta dalle due sezioni seguenti:

- **Panoramica dei carichi di lavoro:** fornisce una panoramica del numero di carichi di lavoro di archiviazione sui cluster ONTAP gestiti da Unified Manager.
- **Panoramica del data center:** fornisce una panoramica della capacità e degli IOPS dei carichi di lavoro di archiviazione nel data center. I dati rilevanti vengono visualizzati a livello di data center e per singolo individuo.

Sezione panoramica dei carichi di lavoro

La sezione Panoramica dei carichi di lavoro fornisce informazioni cumulative e immediate sui carichi di lavoro di archiviazione. Lo stato dei carichi di lavoro di archiviazione viene visualizzato in base ai livelli di servizio delle prestazioni assegnati e non assegnati.

- **Assegnato:** vengono segnalati i seguenti stati per i carichi di lavoro di archiviazione a cui sono stati assegnati livelli di servizio delle prestazioni:
 - **Conforme:** le prestazioni dei carichi di lavoro di archiviazione si basano sui livelli di servizio delle prestazioni loro assegnati. Se i carichi di lavoro di archiviazione rientrano nella latenza di soglia definita nei livelli di servizio delle prestazioni associati, vengono contrassegnati come "conformi". I carichi di lavoro conformi sono contrassegnati in blu.
 - **Non conforme:** durante il monitoraggio delle prestazioni, i carichi di lavoro di archiviazione vengono contrassegnati come "non conformi" se la latenza dei carichi di lavoro di archiviazione supera la latenza di soglia definita nel livello di servizio delle prestazioni associato. I carichi di lavoro non conformi sono contrassegnati in arancione.

- **Non disponibile:** i carichi di lavoro di archiviazione vengono contrassegnati come “non disponibili” se sono offline o se il cluster corrispondente non è raggiungibile. I carichi di lavoro non disponibili sono contrassegnati in rosso.
- **Non assegnato:** i carichi di lavoro di archiviazione a cui non è assegnato un livello di servizio delle prestazioni vengono segnalati come “non assegnati”. Il numero è indicato dall'icona informativa.

Il conteggio totale del carico di lavoro è la somma totale dei carichi di lavoro assegnati e non assegnati.

È possibile fare clic sul numero totale di carichi di lavoro visualizzati in questa sezione e visualizzarli nella pagina Carichi di lavoro.

La sottosezione Conformità per livelli di servizio delle prestazioni visualizza il numero totale di carichi di lavoro di archiviazione disponibili:

- Conforme a ciascun tipo di livello di servizio prestazionale
- Per i quali vi è una discrepanza tra i livelli di servizio prestazionali assegnati e quelli consigliati

Sezione panoramica del data center

La sezione Panoramica del data center rappresenta graficamente la capacità disponibile e utilizzata, nonché gli IOPS per tutti i cluster nel data center. Utilizzando questi dati, dovresti gestire la capacità e gli IOPS dei carichi di lavoro di archiviazione. La sezione visualizza anche le seguenti informazioni per i carichi di lavoro di archiviazione in tutti i cluster:

- La capacità totale, disponibile e utilizzata per tutti i cluster nel tuo data center
- Gli IOPS totali, disponibili e utilizzati per tutti i cluster nel tuo data center
- La capacità disponibile e utilizzata in base a ciascun livello di servizio prestazionale
- Gli IOPS disponibili e utilizzati in base a ciascun livello di servizio prestazionale
- Lo spazio totale e gli IOPS utilizzati dai carichi di lavoro a cui non è assegnato alcun livello di servizio di prestazioni

Come vengono calcolate la capacità e le prestazioni del data center in base ai livelli di servizio delle prestazioni

La capacità utilizzata e gli IOPS vengono recuperati in termini di capacità totale utilizzata e prestazioni di tutti i carichi di lavoro di storage nei cluster.

Gli IOPS disponibili vengono calcolati in base alla latenza prevista e ai livelli di servizio delle prestazioni consigliati sui nodi. Include gli IOPS disponibili per tutti i livelli di servizio delle prestazioni la cui latenza prevista è inferiore o uguale alla propria latenza prevista.

La capacità disponibile viene calcolata in base alla latenza prevista e ai livelli di servizio delle prestazioni consigliati sugli aggregati. Include la capacità disponibile per tutti i livelli di servizio delle prestazioni la cui latenza prevista è inferiore o uguale alla propria latenza prevista.

Visualizza i carichi di lavoro

Quando si aggiungono cluster a Unified Manager, i carichi di lavoro di archiviazione su ciascun cluster vengono automaticamente rilevati e visualizzati nella pagina Carichi di lavoro.

Unified Manager inizia ad analizzare i carichi di lavoro per ottenere raccomandazioni (PSL consigliati) solo

dopo l'avvio delle operazioni di I/O sui carichi di lavoro di archiviazione.

Sono esclusi i volumi FlexGroup e i suoi componenti.

Panoramica dei carichi di lavoro

La pagina Panoramica carichi di lavoro mostra una panoramica dei carichi di lavoro nel data center, nonché una panoramica dello spazio e delle prestazioni del data center.

- Pannello **Panoramica carichi di lavoro**: mostra il numero totale di carichi di lavoro e il numero di carichi di lavoro con o senza PSL assegnati. Viene inoltre visualizzata la ripartizione del conteggio del carico di lavoro per ogni PSL. Facendo clic sui conteggi si accede alla visualizzazione **Tutti i carichi di lavoro** con i carichi di lavoro filtrati. È anche possibile visualizzare il numero di carichi di lavoro non conformi alle raccomandazioni del sistema e assegnare loro i PSL consigliati dal sistema facendo clic sul pulsante **Assegna PSL consigliati dal sistema**.
- Pannello **Panoramica del data center**: mostra lo spazio disponibile e utilizzato (TiB) e le prestazioni (IOPS) del data center. Viene inoltre visualizzata una ripartizione dello spazio disponibile e utilizzato (TiB) e delle prestazioni (IOPS) di tutti i carichi di lavoro in ciascun PSL.

Visualizzazione di tutti i carichi di lavoro

Nella pagina **Archiviazione > Carichi di lavoro > Tutti i carichi di lavoro** sono elencati i carichi di lavoro di archiviazione associati ai cluster ONTAP gestiti da Unified Manager.

Per i carichi di lavoro di archiviazione appena scoperti sui quali non sono state eseguite operazioni di I/O, lo stato è "In attesa di I/O". Dopo l'inizio delle operazioni di I/O sui carichi di lavoro di archiviazione, Unified Manager avvia l'analisi e lo stato del carico di lavoro cambia in "Apprendimento...". Una volta completata l'analisi (entro 24 ore dall'inizio delle operazioni di I/O), vengono visualizzati i PSL consigliati per i carichi di lavoro di archiviazione.

La pagina consente inoltre di assegnare criteri di efficienza di archiviazione (SEP) e livelli di servizio delle prestazioni (PSL) ai carichi di lavoro di archiviazione. È possibile eseguire più attività:

- Aggiungere o predisporre carichi di lavoro di archiviazione
- Visualizza e filtra l'elenco dei carichi di lavoro
- Assegnare PSL ai carichi di lavoro di archiviazione
- Valutare i PSL consigliati dal sistema e assegnarli ai carichi di lavoro
- Assegnare SEP ai carichi di lavoro di archiviazione

Aggiunta o provisioning di carichi di lavoro di archiviazione

È possibile aggiungere o predisporre i carichi di lavoro di archiviazione su LUN supportate (che supportano sia i protocolli iSCSI che FCP), condivisioni file NFS e condivisioni SMB.

Passi

1. Fare clic su **Archiviazione > Carichi di lavoro > Tutti i carichi di lavoro > Crea**.
2. Creare carichi di lavoro. Per informazioni, vedere ["Provisioning e gestione dei carichi di lavoro"](#).

Visualizzazione e filtraggio dei carichi di lavoro

Nella schermata Tutti i carichi di lavoro, puoi visualizzare tutti i carichi di lavoro nel tuo data center o cercare carichi di lavoro di archiviazione specifici in base ai loro PSL o nomi. Puoi utilizzare l'icona del filtro per inserire

condizioni specifiche per la tua ricerca. È possibile effettuare la ricerca in base a diverse condizioni di filtro, ad esempio in base al cluster host o alla VM di archiviazione. L'opzione **Capacità totale** consente di filtrare in base alla capacità totale dei carichi di lavoro (per MB). Tuttavia, in questo caso, il numero di carichi di lavoro restituiti potrebbe variare, perché la capacità totale viene confrontata a livello di byte.

Per ogni carico di lavoro vengono visualizzate informazioni quali il cluster host e la VM di archiviazione, insieme al PSL e al SEP assegnati.

La pagina consente inoltre di visualizzare i dettagli delle prestazioni di un carico di lavoro. È possibile visualizzare informazioni dettagliate su IOPS, capacità e latenza del carico di lavoro facendo clic sul pulsante **Scegli/Ordina colonne** e selezionando le colonne specifiche da visualizzare. La colonna Visualizzazione prestazioni mostra gli IOPS medi e di picco per un carico di lavoro ed è possibile fare clic sull'icona dell'analizzatore del carico di lavoro per visualizzare l'analisi dettagliata degli IOPS.

Analisi dei criteri di prestazioni e capacità per un carico di lavoro

Il pulsante **Analizza carico di lavoro** nel pop-up **Analisi IOPS** conduce alla pagina Analisi carico di lavoro, dove è possibile selezionare un intervallo di tempo e visualizzare i trend di latenza, produttività 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 tramite l'analizzatore dei carichi di lavoro"](#).

È possibile visualizzare informazioni sulle prestazioni di un carico di lavoro per facilitare la risoluzione dei problemi facendo clic sull'icona del grafico a barre nella colonna **Visualizzazione prestazioni**. Per visualizzare i grafici delle prestazioni e della capacità nella pagina Analisi del carico di lavoro per analizzare l'oggetto, fare clic sul pulsante **Analizza carico di lavoro**.

Per maggiori informazioni, vedere ["Quali dati visualizza l'analizzatore del carico di lavoro?"](#).

Assegnare policy ai carichi di lavoro

È possibile assegnare criteri di efficienza di archiviazione (SEP) e livelli di servizio delle prestazioni (PSL) ai carichi di lavoro di archiviazione dalla pagina Tutti i carichi di lavoro utilizzando le diverse opzioni di navigazione.

Assegnare policy a un singolo carico di lavoro

È possibile assegnare un PSL o un SEP o entrambi a un singolo carico di lavoro. Segui questi passaggi:

1. Selezionare il carico di lavoro.
2. Fare clic sull'icona di modifica accanto alla riga, quindi fare clic su **Modifica**.

I campi **Livello di servizio delle prestazioni assegnato** e **Criterio di efficienza dell'archiviazione** sono abilitati.

3. Selezionare il PSL o il SEP desiderato, oppure entrambi.
4. Fare clic sull'icona di controllo per applicare le modifiche.



È anche possibile selezionare un carico di lavoro e fare clic su **Altre azioni** per assegnare i criteri.

Assegna policy a più carichi di lavoro di archiviazione

È possibile assegnare un PSL o un SEP a più carichi di lavoro di archiviazione contemporaneamente. Segui

questi passaggi:

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 di prestazione**. Per assegnare un SEP, selezionare **Assegna policy di efficienza di archiviazione**. Verrà visualizzata una finestra pop-up in cui potrai selezionare la policy.
4. Selezionare la policy appropriata e fare clic su **Applica**. Viene visualizzato il numero di carichi di lavoro a cui sono assegnate le policy. Vengono elencati anche i carichi di lavoro a cui non sono assegnate le policy, con la relativa causa.



L'applicazione di policy in blocco sui carichi di lavoro 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 visualizzarne lo stato di completamento. Se si applica un PSL a più carichi di lavoro, non è possibile attivare un'altra richiesta quando è in esecuzione il precedente processo di assegnazione in blocco.

Assegnare PSL consigliati dal sistema ai carichi di lavoro

È possibile assegnare PSL consigliati dal sistema ai carichi di lavoro di archiviazione in un data center a cui non sono assegnati PSL oppure i PSL assegnati non corrispondono alle raccomandazioni del sistema. Per utilizzare questa funzionalità, fare clic sul pulsante **Assegna PSL consigliati dal sistema**. Non è necessario selezionare carichi di lavoro specifici.

La raccomandazione è determinata internamente dall'analisi del sistema e viene ignorata per quei carichi di lavoro i cui IOPS e altri parametri non coincidono con le definizioni di alcun PSL disponibile. Carichi di lavoro di archiviazione con *Waiting for I/O* e sono esclusi anche gli stati di apprendimento.



Ci sono parole chiave speciali che Unified Manager cerca nel nome del carico di lavoro per sovrascrivere l'analisi del sistema e consigliare un PSL diverso per il carico di lavoro. Quando il carico di lavoro contiene le lettere "ora" nel nome, si consiglia il PSL **Extreme Performance**. E quando il carico di lavoro ha le lettere "vm" nel nome, è consigliato **PerformancePSL**.

Vedi anche l'articolo della knowledge base (KB) ["ActiveIQ Unified Manager 'Assegna il livello di servizio delle prestazioni consigliato dal sistema' non è adattabile a un carico di lavoro altamente variabile"](#)

Fornire volumi di condivisione file

È possibile creare volumi di condivisione file che supportano i protocolli CIFS/SMB e NFS su un cluster esistente e su una macchina virtuale di archiviazione (VM di archiviazione) dalla pagina Provision Workload.

Prima di iniziare

- La VM di archiviazione deve disporre di spazio per il provisioning del volume di condivisione file.
- Uno o entrambi i servizi SMB e NFS devono essere abilitati sulla VM di archiviazione.
- Per selezionare e assegnare il Performance Service Level (PSL) e la Storage Efficiency Policy (SEP) al carico di lavoro, è necessario che le policy siano state create prima di iniziare a creare il carico di lavoro.

Passi

1. Nella pagina **Provision Workload**, aggiungi il nome del carico di lavoro che desideri creare, quindi seleziona il cluster dall'elenco disponibile.
2. In base al cluster selezionato, il campo **STORAGE VM** filtra le VM di archiviazione disponibili per quel cluster. Selezionare la VM di archiviazione richiesta dall'elenco.

In base ai servizi SMB e NFS supportati sulla VM di archiviazione, l'opzione NAS è abilitata nella sezione Informazioni host.

3. Nella sezione Archiviazione e ottimizzazione, assegnare la capacità di archiviazione e il PSL e, facoltativamente, un SEP per il carico di lavoro.

Le specifiche per il SEP vengono assegnate al LUN e le definizioni per il PSL vengono applicate al carico di lavoro al momento della sua creazione.

4. Selezionare la casella di controllo **Applica limiti di prestazioni** se si desidera applicare il PSL assegnato al carico di lavoro.

L'assegnazione di un PSL a un carico di lavoro garantisce che l'aggregato su cui viene creato il carico di lavoro possa supportare gli obiettivi di prestazioni e capacità definiti nella rispettiva policy. Ad esempio, se a un carico di lavoro viene assegnato il PSL "Prestazioni estreme", l'aggregato su cui deve essere eseguito il provisioning del carico di lavoro deve essere in grado di supportare gli obiettivi di prestazioni e capacità della policy "Prestazioni estreme", come l'archiviazione SSD.



Se non si seleziona questa casella di controllo, il PSL non viene applicato al carico di lavoro e lo stato del carico di lavoro nella dashboard appare come non assegnato.

5. Selezionare l'opzione **NAS**.

Se non riesci a vedere l'opzione **NAS** abilitata, verifica se la VM di archiviazione selezionata supporta SMB o NFS, oppure entrambi.



Se la VM di archiviazione è abilitata per i servizi SMB e NFS, è possibile selezionare le caselle di controllo **Condividi tramite NFS** e **Condividi tramite SMB** e creare una condivisione file che supporti entrambi i protocolli NFS e 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.

Aggiungendo l'indirizzo IP dell'host, viene eseguito un controllo interno per verificare la corrispondenza dei dettagli dell'host con la VM di archiviazione e viene creata la policy di esportazione per quell'host oppure, se esiste già una policy, questa viene riutilizzata. Se sono state create più condivisioni NFS per lo stesso host, per tutte le condivisioni di file viene riutilizzata una policy di esportazione disponibile per lo stesso host con regole corrispondenti. La funzione di specificare le regole delle singole policy o di riutilizzare le policy fornendo chiavi policy specifiche è disponibile quando si esegue il provisioning della condivisione NFS tramite API.

7. Per una condivisione SMB, specificare quali utenti o gruppi di utenti possono accedere alla condivisione SMB e assegnare le autorizzazioni necessarie. Per ogni gruppo di utenti, durante la creazione della condivisione file viene generato un nuovo elenco di controllo degli accessi (ACL).
8. Fare clic su **Salva**.

Il carico di lavoro viene aggiunto all'elenco dei carichi di lavoro di archiviazione.

Fornitura di LUN

È possibile creare LUN che supportano i protocolli CIFS/SMB e NFS su un cluster esistente e su una macchina virtuale di archiviazione (VM di archiviazione) dalla pagina Provision Workload.

Prima di iniziare

- La VM di archiviazione deve disporre di spazio per il provisioning della LUN.
- Sia iSCSI che FCP devono essere abilitati sulla VM di archiviazione su cui si crea il LUN.
- Per selezionare e assegnare il Performance Service Level (PSL) e la Storage Efficiency Policy (SEP) al carico di lavoro, è necessario che le policy siano state create prima di iniziare a creare il carico di lavoro.

Passi

1. Nella pagina **Provision Workload**, aggiungi il nome del carico di lavoro che desideri creare, quindi seleziona il cluster dall'elenco disponibile.

In base al cluster selezionato, il campo **STORAGE VM** filtra le VM di archiviazione disponibili per quel cluster.

2. Selezionare dall'elenco la VM di archiviazione che supporta i servizi iSCSI e FCP.

In base alla selezione effettuata, l'opzione SAN viene abilitata nella sezione Informazioni host.

3. Nella sezione **Archiviazione e ottimizzazione**, assegnare la capacità di archiviazione e il PSL e, facoltativamente, l'SEP per il carico di lavoro.

Le specifiche per il SEP vengono assegnate al LUN e le definizioni per il PSL vengono applicate al carico di lavoro al momento della sua creazione.

4. Selezionare la casella di controllo **Applica limiti di prestazioni** se si desidera applicare il PSL assegnato al carico di lavoro.

L'assegnazione di un PSL a un carico di lavoro garantisce che l'aggregato su cui viene creato il carico di lavoro possa supportare gli obiettivi di prestazioni e capacità definiti nella rispettiva policy. Ad esempio, se a un carico di lavoro viene assegnato il PSL "Prestazioni estreme", l'aggregato su cui deve essere eseguito il provisioning del carico di lavoro deve essere in grado di supportare gli obiettivi di prestazioni e capacità della policy "Prestazioni estreme", come l'archiviazione 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 sul dashboard appare come `unassigned`.

5. Selezionare l'opzione **SAN**. Se non riesci a vedere l'opzione **SAN** abilitata, verifica se la VM di archiviazione selezionata supporta iSCSI e FCP.
6. Selezionare il sistema operativo host.
7. Specificare la mappatura host per controllare l'accesso degli iniziatori alla LUN. È possibile assegnare gruppi di iniziatori esistenti (igroup) oppure definire e mappare nuovi igroup.



Se si crea un nuovo igroup durante il provisioning della 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 degli igroup disponibili.

Se si desidera creare un nuovo igroup, selezionare il pulsante **Crea un nuovo gruppo iniziatore** e immettere le informazioni per l'igroup.

8. Fare clic su **Salva**.

La LUN viene aggiunta all'elenco dei carichi di lavoro di archiviazione.

Livelli di servizio prestazionali

Un Performance Service Level (PSL) consente di definire gli obiettivi di prestazioni e archiviazione per un carico di lavoro. È possibile assegnare un PSL a un carico di lavoro durante la creazione iniziale del carico di lavoro oppure in seguito modificandolo.

La gestione e il monitoraggio delle risorse di storage si basano sugli obiettivi del livello di servizio (SLO). Gli SLO sono definiti da accordi sul livello di servizio basati sulle prestazioni e sulla capacità richieste. In Unified Manager, gli SLO fanno riferimento alle definizioni PSL delle applicazioni in esecuzione sullo storage NetApp. I servizi di archiviazione si differenziano in base alle prestazioni e all'utilizzo delle risorse sottostanti. Un PSL è una descrizione degli obiettivi del servizio di archiviazione. Un PSL consente al fornitore di storage di specificare gli obiettivi di prestazioni 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 prestazioni e capacità. Ogni PSL è regolato da IOP di picco, previsti e minimi assoluti, nonché dalla 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:

- Prestazioni estreme
- Prestazione
- Valore

Gli standard PSL Extreme Performance, Performance e Value sono applicabili alla maggior parte dei carichi di lavoro di archiviazione più comuni in un data center.

Unified Manager offre inoltre tre livelli di servizio prestazionali per le applicazioni di database. Si tratta di PSL ad altissime prestazioni che supportano IOPS a raffica e sono adatti per applicazioni di database con la massima richiesta di throughput.

- Extreme per i registri del database
- Extreme per dati condivisi del database
- Estremo per i dati del database
- **Definito dall'utente:** se i livelli di servizio delle prestazioni predefiniti non soddisfano i tuoi requisiti, puoi creare nuovi PSL per soddisfare le tue esigenze. Per informazioni, vedere ["Creare e modificare i livelli di servizio delle prestazioni"](#).
- **Beyond Extreme:** i PSL Beyond Extreme sono i PSL consigliati dal sistema, indicati per carichi di lavoro che richiedono IOP superiori a Extreme. I carichi di lavoro vengono analizzati internamente in base a

IOPS, capacità e latenza e per ciascuno di questi carichi di lavoro si consiglia un Beyond Extreme PSL nella schermata **Archiviazione > Carichi di lavoro > Tutti i carichi di lavoro**. È possibile applicare i PSL ai carichi di lavoro per garantire prestazioni ottimali.

I parametri IOP 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 che un carico di lavoro ha il picco e gli IOP previsti come 106345 E 37929 rispettivamente, il Beyond Extreme PSL generato per il carico di lavoro è denominato `Beyond Extreme 106345 37929`. Sebbene questi PSL siano consigliati dal sistema, quando li assegna ai carichi di lavoro, questi PSL vengono etichettati come `User-defined` nel tipo.

Gestire i carichi di lavoro assegnando PSL

È possibile accedere ai PSL dalla pagina **Politiche > Livelli di servizio delle prestazioni** e utilizzando le API del provider di storage. Gestire i carichi di lavoro di archiviazione assegnando loro dei PSL è comodo, poiché non è necessario gestirli singolarmente. Eventuali modifiche possono essere gestite anche riassegnando un altro PSL anziché gestirli singolarmente. Unified Manager ti aiuta ad assegnare PSL ai tuoi carichi di lavoro in base a valutazioni e raccomandazioni interne.

Per informazioni sull'assegnazione di PSL consigliati dal sistema ai carichi di lavoro, vedere ["Assegnare PSL consigliati dal sistema ai carichi di lavoro"](#)

La pagina Livelli di servizio delle prestazioni 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.

Questa pagina visualizza le seguenti informazioni:

Campo	Descrizione
Nome	Nome del PSL.
Tipo	Se la policy è definita dal sistema o dall'utente.
IOPS/TB previsti	Numero minimo di IOPS che un'applicazione deve eseguire su una LUN o una condivisione file. IOPS previsti specifica il numero minimo di IOPS previsti allocati, in base alle dimensioni allocate dell'oggetto di archiviazione.

Campo	Descrizione
Picco IOPS/TB	Numero massimo di IOPS che un'applicazione può eseguire su una LUN o una condivisione file. Peak IOPS specifica il massimo numero possibile di IOPS allocati, in base alla dimensione dell'oggetto di archiviazione allocato o alla dimensione dell'oggetto di archiviazione utilizzato. I picchi IOPS si basano su una politica di allocazione. La politica di allocazione è quella dello spazio allocato o dello spazio utilizzato. Quando la policy di allocazione è impostata su allocated-space, il picco di IOPS viene calcolato in base alle dimensioni dell'oggetto di archiviazione. Quando la politica di allocazione è impostata su used-space, il picco di IOPS viene calcolato in base alla quantità di dati archiviati nell'oggetto di archiviazione, tenendo conto dell'efficienza di archiviazione. Per impostazione predefinita, la politica di allocazione è impostata su used-space.
IOPS minimo assoluto	Il valore minimo assoluto di IOPS viene utilizzato come override quando il valore di IOPS previsto è inferiore a questo valore. I valori predefiniti dei PSL definiti dal sistema sono i seguenti: • Prestazioni estreme: se IOPS previsti $\geq 6144/\text{TB}$, allora IOPS minimi assoluti = 1000 • Prestazioni: se IOPS previsti $\geq 2048/\text{TB}$ e $< 6144/\text{TB}$, allora IOPS minimi assoluti = 500 • Valore: se IOPS previsti $\geq 128/\text{TB}$ e $< 2048/\text{TB}$, allora IOPS minimi assoluti = 75 I valori predefiniti dei PSL del database definiti dal sistema sono i seguenti: • Estremo per i registri del database: se IOPS previsti ≥ 22528, allora IOPS minimi assoluti = 4000 • Estremo per i dati condivisi del database: se IOPS previsti ≥ 16384, allora IOPS minimi assoluti = 2000 • Estremo per i dati del database: se IOPS previsti ≥ 12288, allora IOPS minimi assoluti = 2000 Il valore massimo degli IOPS minimi assoluti per i PSL personalizzati può essere pari a 75000. Il valore inferiore viene calcolato come segue: 1000/latenza prevista

Campo	Descrizione
Latenza prevista	Latenza prevista per gli IOPS di archiviazione in millisecondi per operazione (ms/op).
Capacità	Capacità totale disponibile e utilizzata nei cluster.
Carichi di lavoro	Numero di carichi di lavoro di archiviazione a cui è stato assegnato il PSL.

Per informazioni su come gli IOPS di picco e gli IOPS previsti contribuiscono a ottenere prestazioni differenziate coerenti sui cluster ONTAP , consultare 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["Che cos'è il Performance Budgeting?"]

Eventi generati per carichi di lavoro che superano la soglia definita dai PSL

Tieni presente 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 avvisarti di un potenziale problema di prestazioni:

- Soglia di latenza del volume del carico di lavoro violata come definito dalla politica sul livello di servizio delle prestazioni
- Soglia di latenza LUN del carico di lavoro violata come definito dalla Performance Service Level Policy.

Potrebbe essere opportuno analizzare il carico di lavoro per vedere cosa potrebbe causare i valori di latenza più elevati.

Per maggiori informazioni, consultare i seguenti ["Eventi di volume"](#)

* ["Cosa succede quando viene violata una soglia di prestazione"](#)

* ["Come Unified Manager utilizza la latenza del carico di lavoro per identificare i problemi di prestazioni"](#)

* ["Quali sono gli eventi di performance"](#)

PSL definiti dal sistema

La tabella seguente fornisce informazioni sui PSL definiti dal sistema:

Livello di servizio delle prestazioni	Descrizione e caso d'uso	Latenza prevista (ms/op)	IOPS di picco	IOPS previsti	IOPS minimo assoluto
Prestazioni estreme	Fornisce una produttività estremamente elevata con una latenza molto bassa Ideale per applicazioni sensibili alla latenza	1	12288	6144	1000

Livello di servizio delle prestazioni	Descrizione e caso d'uso	Latenza prevista (ms/op)	IOPS di picco	IOPS previsti	IOPS minimo assoluto
Prestazione	Fornisce un'elevata produttività a bassa latenza Ideale per database e applicazioni virtualizzate	2	4096	2048	500
Valore	Fornisce un'elevata capacità di archiviazione 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
Extreme per i registri del database	Fornisce la massima produttività con la latenza più bassa. Ideale per applicazioni di database che supportano i log del database. Questo PSL garantisce la massima produttività perché i log del database sono estremamente dinamici e la registrazione è costantemente richiesta.	1	45056	22528	4000

Livello di servizio delle prestazioni	Descrizione e caso d'uso	Latenza prevista (ms/op)	IOPS di picco	IOPS previsti	IOPS minimo assoluto
Extreme per dati condivisi del database	Fornisce un throughput molto elevato con la latenza più bassa. Ideale per le applicazioni di database: dati archiviati in un archivio dati comune, ma condivisi tra più database.	1	32768	16384	2000
Estremo per i dati del database	Fornisce un throughput elevato con la latenza più bassa. Ideale per dati di applicazioni di database, come informazioni di tabelle di database e metadati.	1	24576	12288	2000

Creazione e modifica dei livelli di servizio delle prestazioni

Quando i livelli di servizio delle prestazioni definiti dal sistema non corrispondono ai requisiti del carico di lavoro, è possibile creare livelli di servizio delle prestazioni personalizzati, ottimizzati per i carichi di lavoro.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione.
- Il nome del livello di servizio delle prestazioni 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 livelli di servizio delle prestazioni personalizzati dalla pagina Livelli di servizio delle prestazioni 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.

Passi

1. Nel riquadro di navigazione a sinistra, in **Impostazioni**, seleziona **Criteri > Livelli di servizio delle prestazioni**.
2. Nella pagina **Livelli di servizio delle prestazioni**, fare clic sul pulsante appropriato a seconda che si desideri creare un nuovo livello di servizio delle prestazioni o modificarne uno esistente.

A...	Segui questi passaggi...
Crea un nuovo livello di servizio delle prestazioni	Fare clic su Aggiungi .
Modifica un livello di servizio di prestazioni esistente	Selezionare un livello di servizio delle prestazioni esistente, quindi fare clic su Modifica .

Viene visualizzata la pagina per aggiungere o modificare un livello di servizio delle prestazioni.

3. Personalizza il livello di servizio delle prestazioni specificando gli obiettivi di prestazione, quindi fai clic su **Invia** per salvare il livello di servizio delle prestazioni.

È possibile applicare il nuovo o modificato Performance Service Level ai carichi di lavoro (LUN, condivisioni file NFS, condivisioni CIFS) dalla pagina Carichi di lavoro o durante il provisioning di un nuovo carico di lavoro.

Gestire le policy di efficienza dello storage

Una politica di efficienza di archiviazione (SEP) consente di definire le caratteristiche di efficienza di archiviazione di un carico di lavoro. È possibile assegnare un SEP a un carico di lavoro durante la creazione iniziale del carico di lavoro oppure in seguito modificandolo.

L'efficienza dello storage prevede l'utilizzo di tecnologie quali thin provisioning, deduplicazione e compressione dei dati che aumentano l'utilizzo dello storage e ne riducono i costi. Durante la creazione di SEP, è possibile utilizzare queste tecnologie salvaspazio singolarmente o insieme per ottenere la massima efficienza di archiviazione. Quando si associano i criteri ai carichi di lavoro di archiviazione, vengono loro assegnate le impostazioni dei criteri specificati. Unified Manager consente di assegnare SEP definiti dal sistema e dall'utente per ottimizzare le risorse di storage nel data center.

Unified Manager fornisce due SEP definiti dal sistema: Alto e Basso. Questi SEP sono applicabili alla maggior parte dei carichi di lavoro di archiviazione in un data center; tuttavia, è possibile creare policy personalizzate se gli SEP definiti dal sistema non soddisfano i requisiti.

Non è possibile modificare un SEP definito dal sistema o attualmente assegnato a un carico di lavoro. Non è possibile eliminare un SEP assegnato a un carico di lavoro o se è l'unico SEP disponibile.

La pagina Criteri di efficienza dell'archiviazione elenca i SEP disponibili e consente di aggiungere, modificare ed eliminare i SEP personalizzati. Questa pagina visualizza le seguenti informazioni:

Campo	Descrizione
Nome	Nome del SEP.
Tipo	Se la policy è definita dal sistema o dall'utente.
Riserva spaziale	Se il volume è sottoposto a thin provisioning o thick provisioning.
Deduplicazione	Se la deduplicazione è abilitata sul carico di lavoro: • Inline: la deduplicazione avviene durante la scrittura sul carico di lavoro • Contesto: la deduplicazione avviene nel carico di lavoro • Disabilita: la deduplicazione è disabilitata sul carico di lavoro
Compressione	Se la compressione dei dati è abilitata sul carico di lavoro: • Inline: la compressione dei dati avviene durante la scrittura sul carico di lavoro • Contesto: la compressione dei dati avviene nel carico di lavoro • Disabilita: la compressione dei dati è disabilitata sul carico di lavoro
Carichi di lavoro	Numero di carichi di lavoro di archiviazione a cui è stato assegnato il SEP

Linee guida per la creazione di una politica di efficienza di archiviazione personalizzata

Se gli SEP esistenti non soddisfano i requisiti dei criteri per i carichi di lavoro di archiviazione, è possibile creare un SEP personalizzato. Tuttavia, si consiglia di provare a utilizzare gli SEP definiti dal sistema per i carichi di lavoro di archiviazione e di creare SEP personalizzati solo se necessario.

È possibile visualizzare l'SEP assegnato ai carichi di lavoro nella pagina Tutti i carichi di lavoro e nella pagina Dettagli volume/integrità. È possibile visualizzare il rapporto di riduzione dei dati a livello di cluster (senza copie Snapshot) in base a queste efficienze di archiviazione nel pannello Capacità della Dashboard e nella vista Capacità: Tutti i cluster.

Creare e modificare i criteri di efficienza dell'archiviazione

Quando i criteri di efficienza dell'archiviazione definiti dal sistema non corrispondono ai requisiti del carico di lavoro, è possibile creare criteri di efficienza dell'archiviazione personalizzati, ottimizzati per i carichi di lavoro.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione.
- Il nome del criterio di efficienza di archiviazione 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 criteri di efficienza di archiviazione personalizzati dalla pagina Criteri di efficienza di archiviazione definendo le caratteristiche di efficienza di archiviazione richieste per le applicazioni che accederanno all'archiviazione.



Non è possibile modificare un criterio di efficienza di archiviazione se è attualmente assegnato a un carico di lavoro.

Passi

1. Nel riquadro di navigazione a sinistra, in **Impostazioni**, seleziona **Criteri > Efficienza di archiviazione**.
2. Nella pagina **Criteri di efficienza di archiviazione**, fare clic sul pulsante appropriato a seconda che si desideri creare un nuovo criterio di efficienza di archiviazione o modificarne uno esistente.

A...	Segui questi passaggi...
Crea una nuova politica di efficienza di archiviazione	Fai clic su Aggiungi
Modifica una politica di efficienza di archiviazione esistente	Seleziona un criterio di efficienza di archiviazione esistente e fai clic su Modifica

Viene visualizzata la pagina per aggiungere o modificare un criterio di efficienza di archiviazione.

3. Personalizzare la politica di efficienza di archiviazione specificando le caratteristiche di efficienza di archiviazione, quindi fare clic su **Invia** per salvare la politica di efficienza di archiviazione.

È possibile applicare la nuova o modificata Storage Efficiency Policy ai carichi di lavoro (LUN, condivisioni file NFS, condivisioni CIFS) dalla pagina Carichi di lavoro o durante il provisioning di un nuovo carico di lavoro.

Gestire e monitorare le configurazioni MetroCluster

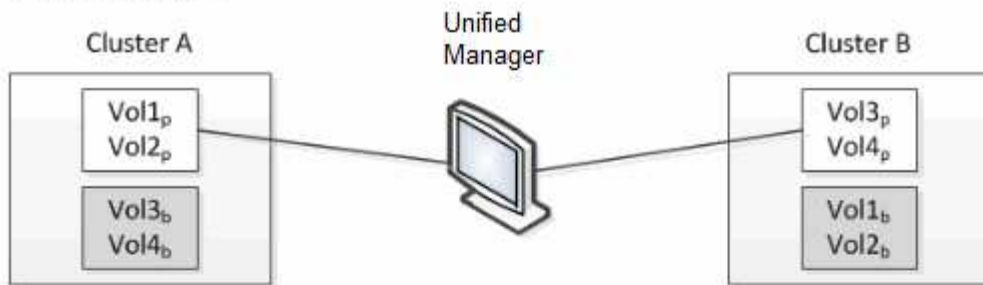
Il supporto di monitoraggio per le configurazioni MetroCluster nell'interfaccia utente Web di Unified Manager consente di verificare eventuali problemi di connettività nelle configurazioni MetroCluster su FC e IP. Individuare tempestivamente un problema di connettività consente di gestire in modo efficace le configurazioni MetroCluster .

Comportamento del volume durante la commutazione e la commutazione indietro

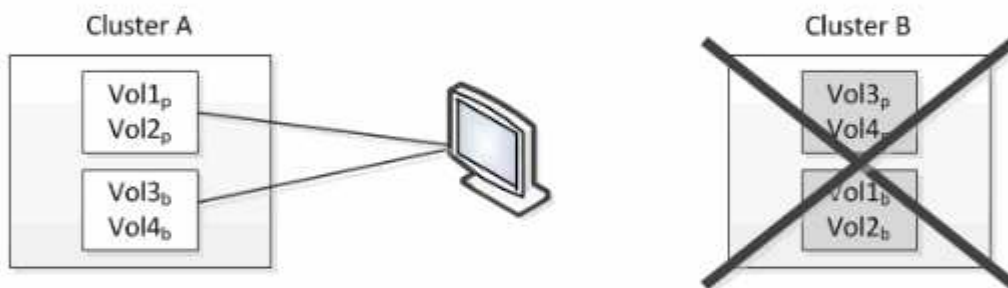
Gli eventi che attivano uno switchover o uno switchback determinano lo spostamento dei volumi attivi da un cluster all'altro nel gruppo di disaster recovery. I volumi sul cluster che erano attivi e fornivano dati ai client vengono arrestati, mentre i volumi sull'altro cluster vengono attivati e iniziano a fornire 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:

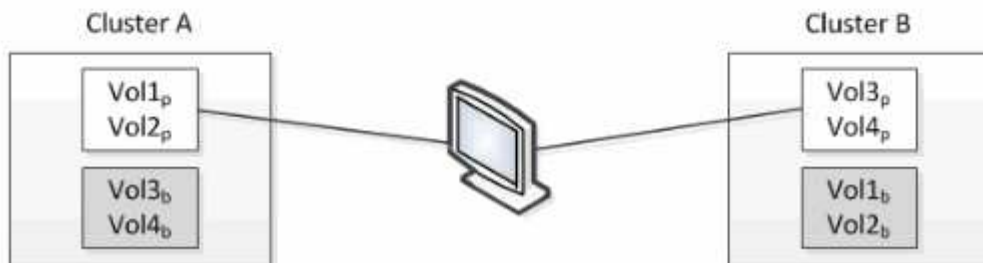
Normal operation



Cluster B fails --- switchover to Cluster A



Cluster B is repaired --- switchback to Cluster B



= active and monitored

= inactive and not monitored

I volumi con la lettera p nel nome indicano i volumi primari, mentre i volumi con la lettera b nel nome sono volumi di backup mirror 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, mentre le statistiche Vol3p e Vol4p vengono raccolte dal Cluster B.

Dopo che un guasto catastrofico provoca il passaggio dei volumi attivi dal Cluster B al Cluster A:

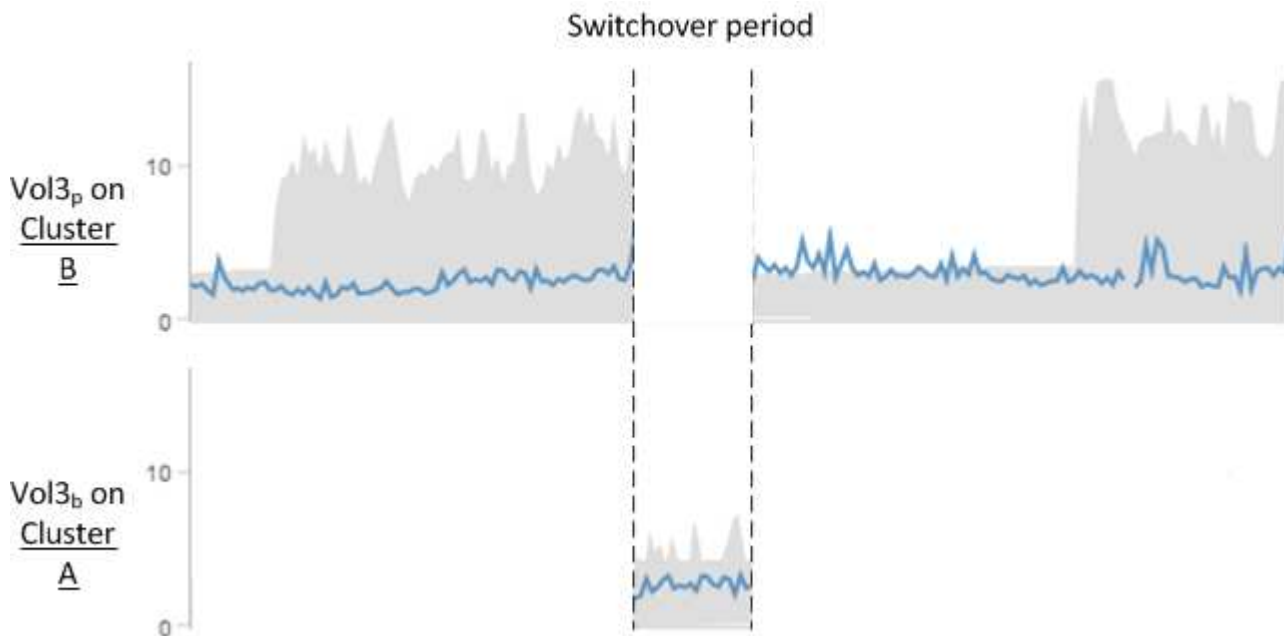
- Il cluster A ha quattro volumi attivi: Vol1p, Vol2p, Vol3b e Vol4b.
- Il cluster B ha quattro volumi inattivi: Vol3p, Vol4p, Vol1b e Vol2b.

Come durante il normale funzionamento, le informazioni relative a ciascuno dei volumi attivi vengono raccolte da Unified Manager. Ma in questo caso, le statistiche Vol1p e Vol2p vengono raccolte dal Cluster A, e anche le statistiche Vol3b e Vol4b vengono raccolte dal Cluster A.

Si noti che Vol3p e Vol3b non sono gli stessi volumi, perché si trovano su cluster diversi. Le informazioni in Unified Manager per Vol3p non sono le stesse di Vol3b:

- Durante il passaggio al Cluster A, le statistiche e gli eventi Vol3p non sono visibili.
- Già al primo passaggio, il Vol3b appare come un nuovo volume privo di informazioni storiche.

Quando il Cluster B viene riparato e viene eseguito un switchback, Vol3p è di nuovo attivo sul Cluster B, con le statistiche storiche e un gap di statistiche per il periodo durante lo switchover. Vol3b non è visualizzabile dal Cluster A finché non si verifica un altro passaggio:



- I volumi MetroCluster inattivi, ad esempio Vol3b sul Cluster A dopo lo switchback, vengono identificati con il messaggio “Questo volume è stato eliminato”. Il volume non è stato effettivamente eliminato, ma al momento non è monitorato da Unified Manager perché non è il volume attivo.
- Se un singolo Unified Manager monitora entrambi i cluster in una configurazione MetroCluster, la ricerca del volume restituisce informazioni per il volume attivo in quel momento. Ad esempio, una ricerca per "Vol3" restituirebbe statistiche ed eventi per Vol3b sul Cluster A se si è verificato un passaggio e Vol3 è diventato attivo sul Cluster A.

Definizioni dello stato di connettività del cluster per MetroCluster sulla configurazione FC

La connettività tra i cluster in una configurazione MetroCluster su FC può avere uno dei

seguenti stati: Ottimale, Interessato o Inattivo. La comprensione degli stati di connettività consente di gestire in modo efficace le configurazioni MetroCluster .

Stato di connettività	Descrizione	Icona visualizzata
Ottimale	La connettività tra i cluster nella configurazione MetroCluster è normale.	
Impattato	Uno o più errori compromettono lo stato di disponibilità del failover; tuttavia, entrambi i cluster nella configurazione MetroCluster sono ancora attivi. Ad esempio, quando il collegamento ISL è inattivo, quando il collegamento IP intercluster è inattivo o quando il cluster partner non è raggiungibile.	
Giù	La connettività tra i cluster nella configurazione MetroCluster è interrotta perché uno o entrambi i cluster sono inattivi oppure sono in modalità failover. Ad esempio, quando il cluster partner è inattivo a causa di un disastro o quando è pianificato un passaggio a fini di test.	Commutazione con errori:  Passaggio riuscito: 

Definizioni dello stato di mirroring dei dati per MetroCluster su FC

Le configurazioni MetroCluster su FC forniscono il mirroring dei dati e la possibilità aggiuntiva di avviare un failover se un intero sito diventa non disponibile. 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 di mirroring dei dati	Descrizione	Icona visualizzata
Normale	Il mirroring dei dati tra i cluster nella configurazione MetroCluster è normale.	

Stato di mirroring dei dati	Descrizione	Icona visualizzata
Mirroring non disponibile	Il mirroring dei dati tra i cluster nella configurazione MetroCluster non è disponibile a causa del passaggio. Ad esempio, quando il cluster partner è inattivo a causa di un disastro o quando è pianificato un passaggio a fini di test.	Commutazione con errori:  Passaggio riuscito: 

Monitorare le configurazioni MetroCluster

È possibile monitorare i problemi di connettività nella configurazione MetroCluster . I dettagli includono lo stato dei componenti e la connettività all'interno di un cluster, nonché lo stato della connettività tra i cluster nella configurazione MetroCluster . Qui imparerai come monitorare i problemi di connettività nei cluster protetti dalle configurazioni MetroCluster su FC e MetroCluster su IP.

È possibile monitorare le configurazioni MetroCluster dalle seguenti viste del riquadro di navigazione sinistro Active IQ Unified Manager :

- **Archiviazione > Cluster > Protezione: MetroCluster** visualizza
- **Protezione > Relazioni > Relazione: MetroCluster** visualizza

Unified Manager utilizza avvisi sullo stato del sistema per indicare lo stato dei componenti e della connettività nella configurazione MetroCluster .

Prima di iniziare

- Sia i cluster locali che quelli remoti in una configurazione MetroCluster devono essere aggiunti ad Active IQ Unified Manager.
- In una configurazione MetroCluster su IP, se si desidera supportare un mediatore, è necessario configurarlo e aggiungerlo al cluster tramite l'API corrispondente.
- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Monitora i problemi di connettività in MetroCluster tramite la configurazione FC

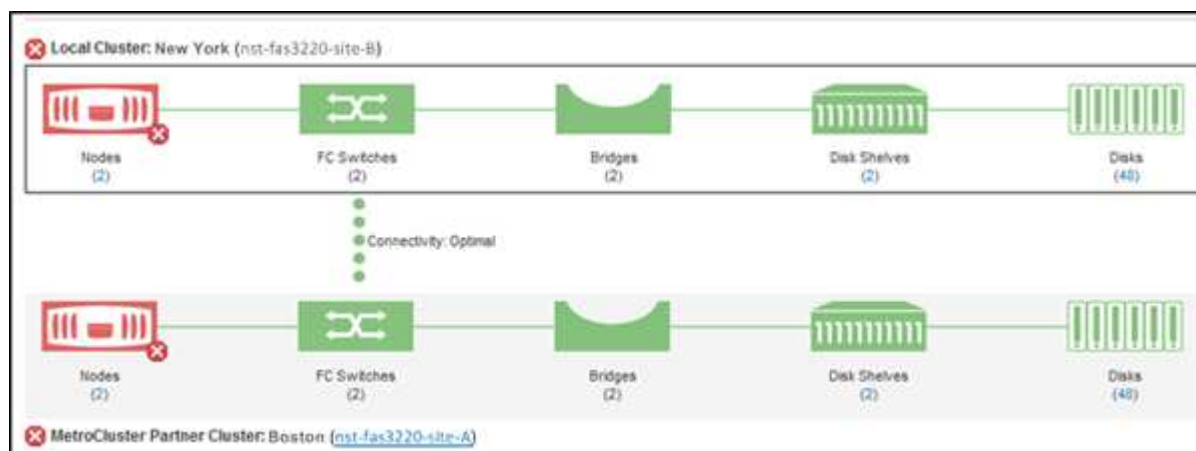
Per i cluster in una configurazione MetroCluster su FC, i grafici di connettività vengono visualizzati nella pagina dei dettagli **Cluster / Integrità**. Seguire questi passaggi.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.

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 per cluster in una configurazione MetroCluster .
3. Nella pagina dei dettagli **Cluster / Salute**, 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 dell'oggetto cluster corrispondente. È possibile utilizzare le informazioni visualizzate nella pagina dei dettagli Cluster/Stato per correggere eventuali problemi di connettività. Ad esempio, se la connettività tra il nodo e lo switch in un cluster non funziona, viene visualizzata la seguente icona:



Se si sposta 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 System Manager o ONTAP CLI per risolvere i problemi.

Per ulteriori informazioni sulla determinazione dello stato di integrità del cluster, vedere ["Determinare lo stato del cluster in MetroCluster tramite la configurazione FC"](#) .

Monitora i problemi di connettività nella configurazione MetroCluster su IP

Per i cluster in una configurazione MetroCluster su IP, i grafici di connettività vengono visualizzati nella pagina **Clusters**. Seguire questi passaggi.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.

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 di MetroCluster su IP. In alternativa, è possibile filtrare per cluster in una configurazione MetroCluster .
3. Espandi la riga cliccando sul cursore ▼ icona. L'icona del cursore appare solo per un cluster protetto da MetroCluster tramite configurazione IP.

È possibile visualizzare la topologia dei siti sorgente e mirror, nonché il mediatore, se presente, utilizzato per la connessione. È possibile visualizzare le seguenti informazioni:

- Connettività tra i siti
- Problemi di salute e disponibilità, se presenti, su entrambi i siti
- Problemi relativi al mediatore
- Problemi relativi alla replicazione.



Vengono segnalati i seguenti stati: Critico (❌), Errore (⚠️), o Normale (✅). È anche possibile visualizzare lo stato di replicazione dei dati aggregati dei dati primari e mirror nella stessa topologia.

Nel diagramma seguente, è possibile vedere che la connettività tra i cluster di origine e di destinazione non è disponibile e il mediatore 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 su IP, è possibile fare clic sul pulsante **Visualizza evento** nel messaggio e visualizzare i dettagli dell'evento. Una volta risolto il problema e l'evento, l'icona di stato in questa topologia torna normale (✅).
5. È possibile visualizzare ulteriori dettagli sulla configurazione nelle sezioni **Panoramica MetroCluster *** e ***Protezione** nella scheda **Configurazione** della pagina dei dettagli **Cluster/Integrità**.



Solo per una configurazione MetroCluster su IP, è possibile visualizzare la topologia del cluster nella pagina **Cluster**. Per i cluster in una configurazione MetroCluster su FC, la topologia viene visualizzata nella scheda **Connettività MetroCluster *** nella pagina dei dettagli ***Cluster / Integrità**.

Informazioni correlate

- ["Pagina dei dettagli del cluster/salute"](#)
- Per informazioni sulla visualizzazione **Relazione: MetroCluster**, vedere ["Monitorare le configurazioni MetroCluster"](#).
- Per informazioni sulla visualizzazione **Relazione: Stato del trasferimento dell'ultimo mese**, vedere ["Relazione: Visualizzazione dello stato del trasferimento dell'ultimo mese"](#).
- Per informazioni sulla visualizzazione **Relazione: Tasso di trasferimento ultimo mese**,

vedere ["Relazione: Visualizzazione del tasso di trasferimento dell'ultimo mese"](#) .

- Per informazioni sulla visualizzazione **Relazione: Tutte le relazioni**, vedere ["Relazione: visualizzazione di tutte le relazioni"](#) .

Monitorare la replica MetroCluster

È possibile monitorare e diagnosticare lo stato di salute generale delle connessioni logiche durante il mirroring dei dati. È possibile identificare i problemi o eventuali rischi che interrompono il mirroring dei componenti del cluster, quali aggregati, nodi e macchine virtuali di archiviazione.

Unified Manager utilizza avvisi sullo stato del sistema per monitorare lo stato dei componenti e la connettività nella configurazione MetroCluster .

Prima di iniziare

Sia il cluster locale che quello remoto nella configurazione MetroCluster devono essere aggiunti a Unified Manager

Visualizza la replica per le configurazioni MetroCluster su IP

Per le configurazioni MetroCluster su IP, lo stato di replicazione dei dati viene visualizzato nella vista panoramica della topologia per un cluster protetto da MetroCluster su IP dalle seguenti viste del riquadro di navigazione sinistro di Unified Manager:

- **Archiviazione > Cluster > Protezione: MetroCluster** visualizza
- **Protezione > Relazioni > Relazione: MetroCluster** visualizza

Per informazioni, vedere ["Monitora i problemi di connettività in MetroCluster su IP"](#) .

Visualizza la replica per le configurazioni MetroCluster su FC

Seguire questi passaggi per determinare eventuali problemi nella replica dei dati per la configurazione MetroCluster su FC.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.

Viene visualizzato un elenco dei cluster monitorati.

2. Dalla vista **Integrità: Tutti i cluster**, fare clic sul nome del cluster per il quale si desidera visualizzare i dettagli della replica 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 dell'oggetto cluster corrispondente, insieme alle informazioni sul sito remoto in cui i dati vengono replicati. Se si sposta il puntatore sull'icona, è possibile visualizzare informazioni dettagliate sull'evento generato.

È possibile utilizzare le informazioni visualizzate nella pagina Dettagli cluster/integrità per correggere eventuali problemi di replica. Se si riscontrano problemi di mirroring nella configurazione MetroCluster , è necessario accedere a System Manager o all'interfaccia CLI ONTAP per risolvere i problemi.

Informazioni correlate

Gestire le quote

È possibile utilizzare 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 informazioni sulle quote degli utenti e dei gruppi di utenti, come l'utilizzo del disco e dei file e i vari limiti impostati sui dischi.

Quali sono i limiti delle quote

I limiti delle quote utente sono valori che il server Unified Manager utilizza per valutare se il consumo di spazio da parte di un utente si sta avvicinando al limite o ha raggiunto il limite impostato dalla quota dell'utente. Se viene superato il limite flessibile o se viene raggiunto il limite rigido, il server Unified Manager genera eventi di quota utente.

Per impostazione predefinita, il server Unified Manager invia un'e-mail di notifica agli utenti che hanno superato il limite flessibile della quota o hanno raggiunto il limite rigido della quota e per i quali sono configurati eventi di quota utente. Gli utenti con il ruolo di amministratore dell'applicazione possono configurare avvisi che notificano ai destinatari specificati gli eventi relativi alle quote utente o gruppo di utenti.

È possibile specificare i limiti di quota utilizzando ONTAP System Manager o ONTAP CLI.

Visualizza le quote degli utenti e dei gruppi di utenti

La pagina Dettagli VM di archiviazione/Stato visualizza informazioni sulle quote utente e gruppo utente configurate sulla SVM. È possibile visualizzare il nome dell'utente o del gruppo di utenti, i limiti impostati sui dischi e sui file, lo spazio su disco e sui file utilizzato e l'indirizzo e-mail per le notifiche.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Nella vista **Integrità: tutte le VM di archiviazione**, seleziona una VM di archiviazione e quindi fai clic sulla scheda **Quote utente e gruppo**.

Informazioni correlate

["Aggiunta di utenti"](#)

Crea regole per generare indirizzi email

È possibile creare regole per specificare l'indirizzo e-mail in base alla quota utente associata a cluster, macchine virtuali di archiviazione (SVM), volumi, qtree, utenti o gruppi di utenti. In caso di violazione della quota, viene inviata una notifica all'indirizzo e-mail specificato.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver esaminato le linee guida nella pagina Regole per generare indirizzi email per quote utente e gruppo.

È necessario definire le regole per gli indirizzi e-mail quotati e inserirle nell'ordine in cui si desidera eseguirle. Ad esempio, se si desidera utilizzare l'indirizzo email abc@xyz.com per ricevere notifiche sulle violazioni delle quote per abc e utilizzare l'indirizzo email di-\$GROUP@\$DOMAIN per tutti gli altri gruppi, le regole devono essere elencate nel seguente ordine:

- se (\$USER == 'abc') allora abc@xyz.com
- se (\$GROUP == *) allora di-\$GROUP@\$DOMAIN

Se nessuno dei criteri per le regole specificate viene soddisfatto, viene utilizzata la regola predefinita:

se (\$USER_OR_GROUP == *) allora \$USER_OR_GROUP@\$DOMAIN

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Regole e-mail per le quote**.
2. Inserisci la regola in base ai tuoi criteri.
3. Fare clic su **Convalida** per convalidare la sintassi della regola.

Se la sintassi della regola non è corretta, viene visualizzato un messaggio di errore. È necessario correggere la sintassi e fare nuovamente clic su **Convalida**.

4. Fare clic su **Salva**.
5. Verifica che l'indirizzo email creato sia visualizzato nella scheda **Quote utente e gruppo** della pagina dei dettagli **VM/Stato** di archiviazione.

Creare un formato di notifica e-mail per le quote degli utenti e dei gruppi di utenti

È possibile creare un formato di notifica per le e-mail inviate a un utente o a un gruppo di utenti quando si verifica un problema relativo alla quota (superamento del limite flessibile o raggiungimento del limite rigido).

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Formato e-mail quota**.
2. Inserisci o modifica i dettagli nei campi **Da**, **Oggetto** e **Dettagli e-mail**.
3. Fare clic su **Anteprima** per visualizzare l'anteprima della notifica e-mail.
4. Fare clic su **Chiudi** per chiudere la finestra di anteprima.
5. Se necessario, modificare il contenuto della notifica e-mail.
6. Fare clic su **Salva**.

Modifica gli indirizzi email delle quote utente e gruppo

È possibile modificare gli indirizzi e-mail in base alla quota utente associata a cluster, macchine virtuali di archiviazione (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 indirizzi e-mail per quote utente e gruppo.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devi aver esaminato il ["linee guida per la creazione di regole"](#).

Se modifichi un indirizzo email, le regole per generare gli indirizzi email delle quote utente e gruppo non saranno più applicabili alla quota. Per inviare le notifiche all'indirizzo email generato dalle regole specificate, è necessario eliminare l'indirizzo email e salvare la modifica.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > SVM**.
2. Nella vista **Integrità: tutte le VM di archiviazione**, selezionare una SVM e quindi fare clic sulla scheda **Quote utente e gruppo**.
3. Fare clic su **Modifica indirizzo e-mail** sotto la riga di schede.
4. Nella finestra di dialogo **Modifica indirizzo email**, eseguire l'azione appropriata:

Se...	Poi...
Desideri che le notifiche vengano inviate all'indirizzo email generato dalle regole specificate	a. Eliminare l'indirizzo email nel campo Indirizzo email. b. Fare clic su Salva. c. Aggiorna il browser premendo F5 per ricaricare la finestra di dialogo Modifica indirizzo email. L'indirizzo email generato dalla regola specificata viene visualizzato nel campo Indirizzo email.
Desideri che le notifiche vengano inviate a un indirizzo email specificato	a. Modificare l'indirizzo email nel campo Indirizzo email. b. Fare clic su Salva. Le regole per generare gli indirizzi email delle quote utente e gruppo non sono più applicabili alla quota.

Scopri di più sulle quote

Comprendere i concetti relativi alle quote ti aiuta a gestire in modo efficiente le quote utente e le quote dei gruppi di utenti.

Panoramica del processo di quota

Le quote possono essere flessibili o rigide. Le quote flessibili fanno sì che ONTAP invii una notifica quando vengono superati i limiti specificati, mentre le quote rigide impediscono che un'operazione di scrittura vada a buon fine quando vengono superati i limiti specificati.

Quando ONTAP riceve una richiesta da un utente o da un gruppo di utenti per scrivere su un FlexVol volume, verifica se le quote sono attivate su quel 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 fallisce quando viene raggiunto il limite massimo e viene inviata la notifica della quota massima.

- Se il limite soft verrà violato

In caso affermativo, l'operazione di scrittura riesce quando il limite flessibile viene superato e viene inviata la notifica della quota flessibile.

- Se un'operazione di scrittura non supererà il limite flessibile

In caso affermativo, l'operazione di scrittura riesce e non viene inviata alcuna notifica.

Informazioni 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. Si specificano le quote utilizzando `/etc/quotas` file. Le quote vengono applicate a un volume o qtree specifico.

Perché si usano le quote

È possibile utilizzare le quote per limitare l'utilizzo delle risorse nei volumi FlexVol , per inviare notifiche quando l'utilizzo delle risorse raggiunge livelli specifici o per monitorare l'utilizzo delle risorse.

Si specifica 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 da 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, gruppo o qtree, senza imporre un limite
- Per avvisare gli utenti quando l'utilizzo del disco o dei file è elevato

Descrizione delle finestre di dialogo delle quote

È possibile utilizzare l'opzione appropriata nella scheda Quote utente e gruppo nella vista Integrità: tutte le VM di archiviazione 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 e-mail

La pagina Formato notifica e-mail visualizza le regole dell'e-mail inviata a un utente o a un gruppo di utenti quando si verifica un problema relativo alla quota (superamento del limite flessibile o raggiungimento del limite rigido).

La notifica e-mail viene inviata solo quando vengono generati i seguenti eventi di quota utente o gruppo di utenti: Violazione del limite flessibile dello spazio su disco della quota utente o gruppo, Violazione del limite flessibile del numero di file della quota utente o gruppo, Raggiunto il limite rigido dello spazio su disco della quota utente o gruppo, oppure Raggiunto il limite rigido del numero di file della quota utente o gruppo.

- **Da**

Visualizza l'indirizzo email da cui viene inviata l'email, che puoi modificare. Per impostazione predefinita, questo è l'indirizzo email specificato nella pagina Notifiche.

- **Soggetto**

Visualizza l'oggetto dell'e-mail di notifica.

- **Dettagli e-mail**

Visualizza il testo dell'e-mail di notifica. Puoi modificare il testo in base alle tue esigenze. Ad esempio, è possibile fornire informazioni relative agli attributi delle quote e ridurre il numero di parole chiave. Tuttavia, non dovresti modificare le parole chiave.

Le parole chiave valide sono le seguenti:

- **\$EVENT_NAME**

Specifica il nome dell'evento che ha causato la notifica via e-mail.

- **\$QUOTA_TARGET**

Specifica il qtree o il volume su cui è applicabile la quota.

- **\$QUOTA_UTILIZZATA_PERCENTUALE**

Specifica la percentuale del limite rigido del disco, del limite flessibile del disco, del limite rigido del file o del limite flessibile del file utilizzata dall'utente o dal gruppo di utenti.

- **\$QUOTA_LIMIT**

Specifica il limite massimo del disco 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 utente o gruppo raggiunto
 - Limite flessibile dello spazio su disco della quota utente o gruppo raggiunto
 - Limite massimo di conteggio file quota utente o gruppo raggiunto
 - Limite flessibile del numero di file di quota utente o gruppo raggiunto

- **\$QUOTA_USED**

Specifica lo spazio su disco utilizzato o il numero di file creati dall'utente o dal gruppo di utenti.

- \$QUOTA_USER

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'e-mail di notifica.

- **Ripristina impostazioni di fabbrica**

Consente di ripristinare il formato di notifica ai valori predefiniti di fabbrica.

- **Salva**

Salva le modifiche apportate al formato di notifica.

Pagina Regole per generare indirizzi email di quote utente e gruppo

La pagina Regole per generare indirizzi e-mail con quote utente e gruppo consente di creare regole per specificare indirizzi e-mail in base alla quota utente associata a cluster, SVM, volumi, qtree, utenti o gruppi di utenti. Quando viene superata una quota, viene inviata una notifica all'indirizzo e-mail specificato.

Area regole

È necessario definire le regole per un indirizzo email con quota. Puoi anche aggiungere commenti per spiegare le regole.

Come definisci le regole

È necessario immettere le regole nell'ordine in cui si desidera eseguirle. Se il criterio della prima regola viene soddisfatto, l'indirizzo email 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 nell'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 email qtree1@xyz.com per ricevere notifiche sulle violazioni delle quote per qtree1 e utilizzare l'indirizzo email admin@xyz.com per tutti gli altri qtree, le regole devono essere elencate nel seguente ordine:

- se (\$QTREE == 'qtree1') 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 \$USER_OR_GROUP@\$DOMAIN

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

Puoi aggiungere commenti per spiegare le regole. Dovresti usare # all'inizio di ogni commento e ogni riga elenca un commento separato.

Sintassi delle regole

La sintassi della regola deve essere una delle seguenti:

- `Se ( valid variableoperator * ) Poi email ID@domain name`

if è una parola chiave ed è scritta in minuscolo. L'operatore è ==. L'ID e-mail può contenere qualsiasi carattere, le variabili valide \$USER_OR_GROUP, \$USER o \$GROUP oppure una combinazione di qualsiasi carattere e le variabili valide \$USER_OR_GROUP, \$USER o \$GROUP. Il nome di dominio può contenere qualsiasi carattere, la variabile valida \$DOMAIN o una combinazione di qualsiasi carattere e della variabile valida \$DOMAIN. Le variabili valide possono essere scritte in maiuscolo o in minuscolo, ma non devono essere una combinazione di entrambe. Ad esempio, \$domain e \$DOMAIN sono validi, ma \$Domain non è una variabile valida.

- `Se ( valid variableoperator `string` ) Poi email ID@domain name`

if è una parola chiave ed è in minuscolo. L'operatore può essere contains o ==. L'ID e-mail può contenere qualsiasi carattere, le variabili valide \$USER_OR_GROUP, \$USER o \$GROUP oppure una combinazione di qualsiasi carattere e le variabili valide \$USER_OR_GROUP, \$USER o \$GROUP. Il nome di dominio può contenere qualsiasi carattere, la variabile valida \$DOMAIN o una combinazione di qualsiasi carattere e della variabile valida \$DOMAIN. Le variabili valide possono essere scritte in maiuscolo o in minuscolo, ma non devono essere una combinazione di entrambe. Ad esempio, \$domain e \$DOMAIN sono validi, ma \$Domain 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. Se si verificano errori durante la convalida, viene visualizzata la regola che ha generato l'errore insieme a un messaggio di errore.

- **Ripristina impostazioni di fabbrica**

Consente di ripristinare le regole degli indirizzi ai valori predefiniti di fabbrica.

- **Salva**

Convalida la sintassi della regola e salva la regola se non ci sono errori. Se si verificano errori durante la convalida, viene visualizzata la regola che ha generato l'errore insieme a un messaggio di errore.

Risoluzione dei problemi

Le informazioni sulla risoluzione dei problemi ti aiutano a identificare e risolvere i problemi che si verificano durante l'utilizzo di Unified Manager.

Aggiungere spazio su disco alla directory del database Unified Manager

La directory del database Unified Manager contiene tutti i dati sullo stato e sulle prestazioni raccolti dai sistemi ONTAP . In alcune circostanze potrebbe essere necessario aumentare le dimensioni della directory del database.

Ad esempio, la directory del database potrebbe riempirsi se Unified Manager raccoglie dati da un numero elevato di cluster, ognuno dei quali ha molti nodi. Riceverai un evento di 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 dati sono diversi a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, su un server Red Hat Linux o su un server Microsoft Windows.

Aggiungere 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 tramite la console di manutenzione di Unified Manager.

Prima di iniziare

- È necessario avere accesso a vSphere Client.
- La macchina virtuale non deve avere snapshot archiviati 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.

Passi

1. Nel client vSphere, seleziona la macchina virtuale Unified Manager, quindi aggiungi più capacità del disco ai dati `disk 3` . Per maggiori dettagli, consultare la documentazione VMware.

In alcuni rari casi la distribuzione di Unified Manager utilizza "Hard Disk 2" per il disco dati anziché "Hard Disk 3". Se questo si è verificato nella distribuzione, aumentare lo spazio del disco più grande. Il disco dati avrà sempre più spazio rispetto all'altro disco.

2. Nel client vSphere, seleziona la macchina virtuale Unified Manager, quindi seleziona la scheda **Console**.
3. Fare clic nella finestra della console, quindi accedere alla console di manutenzione utilizzando il nome utente e la password.
4. Nel **Menu principale**, immettere il numero per l'opzione **Configurazione del sistema**.
5. Nel **Menu di configurazione del sistema**, immettere il numero per l'opzione **Aumenta dimensione disco dati**.

Aggiungere spazio alla directory dati dell'host Linux

Se hai assegnato spazio su disco insufficiente al `/opt/netapp/data` directory per supportare Unified Manager quando hai originariamente configurato l'host Linux e poi installato Unified Manager, puoi aggiungere spazio su disco dopo l'installazione

aumentando lo spazio su disco su `/opt/netapp/data` elenco.

Prima di iniziare

È necessario disporre dell'accesso come utente root al computer Red Hat Enterprise 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.

Passi

1. Accedi come utente root al computer Linux su cui desideri aggiungere spazio su disco.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine mostrato: `systemctl stop ocieau ocie mysqld`
3. Creare una cartella di backup temporanea (ad esempio, `/backup-data`) con spazio su disco sufficiente a contenere i dati nella versione corrente `/opt/netapp/data` elenco.
4. Copia 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 SE Linux è abilitato:

- a. Ottieni il tipo 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 alla seguente:

```
echo $se_type  
mysqld_db_t
```

- a. Esegui il `chcon` comando per impostare il tipo SE Linux per la directory di backup:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Rimuovere il contenuto del `/opt/netapp/data` elenco:

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

7. Espandi le dimensioni del `/opt/netapp/data` directory a un minimo di 150 GB tramite comandi LVM o aggiungendo dischi extra.



Se hai creato `/opt/netapp/data` da un disco, allora non dovresti provare a montarlo `/opt/netapp/data` come quota NFS o CIFS. Perché, in questo caso, se si tenta di espandere lo spazio su disco, alcuni comandi LVM, come `resize` E `extend` potrebbe non funzionare come previsto.

8. Confermare 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 alla seguente:

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. Se SE Linux è abilitato, confermare 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 alla seguente:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0  
/opt/netapp/data/abc
```

10. Elimina il file `abc` in modo che questo file estraneo non causi un errore del database in futuro.

11. Copia il contenuto da `backup-data` torna all'espansione `/opt/netapp/data` elenco:

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

12. Se SE Linux è abilitato, eseguire il seguente comando:

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Avviare il servizio MySQL:

```
systemctl start mysqld
```

14. Dopo aver avviato il servizio MySQL, avviare i servizi `ocie` e `ocieau` nell'ordine mostrato:

```
systemctl start ocie ocieau
```

15. Dopo aver avviato tutti i servizi, eliminare la cartella di backup `/backup-data` :

```
rm -rf /backup-data
```

Aggiungere 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.

Prima di iniziare

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.

Passi

1. Accedi come amministratore al server Windows su cui desideri aggiungere spazio su disco.
2. Segui il passaggio che corrisponde al metodo che vuoi utilizzare per aggiungere più spazio:

Opzione	Descrizione
Su un server fisico, aggiungere capacità all'unità logica su cui è installato il server Unified Manager.	Seguire i passaggi indicati nell'argomento Microsoft: "Estendi un volume di base"
Su un server fisico, aggiungere un'unità disco rigido.	Seguire i passaggi indicati nell'argomento Microsoft: "Aggiunta di unità disco rigido"
Su una macchina virtuale, aumentare le dimensioni di una partizione del disco.	Seguire i passaggi descritti nell'argomento VMware: "Aumento delle dimensioni di una partizione del disco"

Modificare l'intervallo di raccolta delle statistiche sulle prestazioni

L'intervallo di raccolta predefinito per le statistiche sulle prestazioni è di 5 minuti. È possibile modificare questo intervallo a 10 o 15 minuti se si nota che le raccolte provenienti da cluster di grandi dimensioni non vengono completate entro il tempo predefinito. Questa impostazione influisce sulla raccolta di statistiche da tutti i cluster monitorati da questa istanza di Unified Manager.

Prima di iniziare

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 sulle prestazioni che non terminano in tempo è indicato dai messaggi del banner `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>`.

Dovresti modificare l'intervallo di raccolta solo quando necessario a causa di un problema di raccolta delle statistiche. Non modificare questa impostazione per nessun altro motivo.



La modifica di questo valore rispetto all'impostazione predefinita di 5 minuti può influire sul numero e sulla frequenza degli eventi di prestazione segnalati da Unified Manager. Ad esempio, le soglie di prestazioni definite dal sistema attivano eventi quando la policy viene superata per 30 minuti. Quando si utilizzano raccolte di 5 minuti, la norma deve essere superata per sei raccolte consecutive. Per le raccolte di 15 minuti, la norma deve essere superata solo per due periodi di raccolta.

Un messaggio nella parte inferiore della pagina Configurazione cluster indica l'intervallo corrente di raccolta

dei dati statistici.

Passi

1. Accedere tramite SSH come utente di manutenzione all'host Unified Manager.

Vengono visualizzati i prompt della console di manutenzione di Unified Manager.

2. Digitare il numero dell'opzione di menu denominata **Configurazione intervallo di polling delle prestazioni**, quindi premere Invio.
3. Se richiesto, immettere nuovamente la password dell'utente addetto alla manutenzione.
4. Digitare il numero per il nuovo intervallo di polling che si desidera impostare, quindi premere Invio.

Se hai modificato l'intervallo di raccolta di Unified Manager in 10 o 15 minuti e hai una connessione corrente a un provider di dati esterno (ad esempio Graphite), devi modificare l'intervallo di trasmissione del provider di dati in modo che sia uguale o maggiore dell'intervallo di raccolta di Unified Manager.

Modificare la durata del periodo di conservazione dei dati sugli eventi e sulle prestazioni da parte di Unified Manager

Per impostazione predefinita, Unified Manager archivia i dati degli eventi e i dati sulle prestazioni per 6 mesi per tutti i cluster monitorati. Trascorso questo periodo, i dati più vecchi vengono automaticamente eliminati per fare spazio ai nuovi dati. Questo intervallo di tempo predefinito funziona bene per la maggior parte delle configurazioni, ma per configurazioni molto grandi con molti cluster e nodi potrebbe essere necessario ridurre il periodo di conservazione in modo che Unified Manager funzioni in modo ottimale.

Prima di iniziare

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 dei dati. Queste impostazioni influiscono sulla conservazione dei dati di tutti i cluster monitorati da questa istanza di Unified Manager.



Unified Manager raccoglie statistiche sulle prestazioni ogni 5 minuti. Ogni giorno le statistiche di 5 minuti vengono riepilogate in statistiche sulle prestazioni orarie. Conserva 30 giorni di dati storici sulle prestazioni ogni 5 minuti e 6 mesi di dati riepilogativi sulle prestazioni ogni ora (per impostazione predefinita).

Dovresti ridurre il periodo di conservazione solo se lo spazio a disposizione sta per esaurirsi o se il backup e altre operazioni richiedono molto tempo per essere completate. La riduzione del periodo di conservazione ha i seguenti effetti:

- I vecchi dati sulle prestazioni vengono eliminati dal database di Unified Manager dopo mezzanotte.
- I vecchi dati degli eventi vengono eliminati immediatamente dal database di Unified Manager.
- Gli eventi precedenti al periodo di conservazione non saranno più visualizzabili nell'interfaccia utente.
- Le posizioni nell'interfaccia utente in cui vengono visualizzate le statistiche sulle prestazioni orarie saranno vuote prima del periodo di conservazione.
- Se il periodo di conservazione dell'evento supera il periodo di conservazione dei dati sulle prestazioni, verrà visualizzato un messaggio sotto il cursore delle prestazioni, che avvisa che gli eventi sulle prestazioni più vecchi potrebbero non avere dati di supporto nei grafici associati.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Criteri > Conservazione dati**.
2. Nella pagina **Conservazione dati**, seleziona lo strumento cursore nell'area Conservazione eventi o Conservazione dati prestazioni e spostalo sul numero di mesi per cui i dati devono essere conservati, quindi fai clic su **Salva**.

Errore di autenticazione sconosciuto

Quando si esegue un'operazione relativa all'autenticazione, come 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
- Associa il nome distinto del servizio di autenticazione OpenLDAP

Azione correttiva

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. In base al servizio di autenticazione selezionato, immettere le informazioni appropriate per Nome amministratore o Nome distinto di associazione.
3. Fare clic su **Test autenticazione** per testare l'autenticazione con i dettagli specificati.
4. Fare clic su **Salva**.

Utente non trovato

Quando si esegue un'operazione relativa all'autenticazione, come 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 navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Immettere le informazioni appropriate per il nome distinto di base.
3. Fare clic su **Salva**.

Problema con l'aggiunta di LDAP tramite altri servizi di autenticazione

Quando si seleziona Altri come servizio di autenticazione, la classe oggetto dell'utente e del gruppo conserva i valori del modello selezionato in precedenza. 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 dell'oggetto utente LDAP e la classe dell'oggetto gruppo sono rispettivamente `utente` e `gruppo`, procedere come segue:

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Nel menu a discesa **Servizio di autenticazione**, seleziona **Active Directory**, quindi seleziona **Altri**.
3. Completa i campi di testo.

Se la classe dell'oggetto utente LDAP e la classe dell'oggetto gruppo sono rispettivamente `posixAccount` e `posixGroup`, procedere come segue:

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Autenticazione remota**.
2. Nel menu a discesa **Servizio di autenticazione**, seleziona **OpenLDAP**, quindi seleziona **Altri**.
3. Completa i campi di testo.

Se le prime due soluzioni alternative non sono applicabili, chiamare il `option-set API` e impostare il `auth.ldap.userObjectClass` e `auth.ldap.groupObjectClass` opzioni ai valori corretti.

Problema di rotazione dei log di NetApp Manageability SDK sui sistemi Windows

Dopo aver aggiunto un cluster basato su API ONTAPI a Unified Manager su un sistema operativo Windows, `nmsdk.log` la dimensione del file aumenta e supera il limite di 10 MB.

Causa

Questo problema può verificarsi se non si verifica la rotazione del registro.

Azione correttiva

1. Arrestare Unified Manager.
2. Quando si installa Unified Manager su Windows, installare Logrotate versione 0.0.0.18. Per maggiori informazioni, vedere il ["Guida al rafforzamento della sicurezza per il report tecnico di NetApp Manageability SDK"](#).
3. Avviare Unified Manager.

Gestisci eventi e avvisi

Gestire gli eventi

Gli eventi aiutano a identificare i problemi nei cluster monitorati.

Cosa 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 sui messaggi AutoSupport generati da tutti i sistemi di archiviazione monitorati da Unified Manager.

Per maggiori informazioni, vedere ["Come vengono generati gli eventi della piattaforma Active IQ"](#).

Unified Manager verifica automaticamente la presenza di un nuovo file di regole e scarica un nuovo file solo quando sono presenti regole più recenti. Nei siti senza accesso alla rete esterna, è necessario caricare manualmente le regole da **Gestione archiviazione > Configurazione evento > Carica regole**.

Questi eventi Active IQ non si sovrappongono agli eventi Unified Manager esistenti e identificano incidenti o rischi relativi alla configurazione del sistema, al cablaggio, alle best practice e ai problemi di disponibilità.

Per ulteriori informazioni sull'abilitazione degli eventi della piattaforma, vedere ["Abilitazione degli eventi del portale Active IQ"](#) . Per ulteriori informazioni sul caricamento del file delle regole, vedere ["Caricamento di un nuovo file di regole Active IQ"](#) .

NetApp Active IQ è un servizio basato su cloud che fornisce analisi predittive e supporto proattivo per ottimizzare le operazioni del sistema di storage nel cloud ibrido NetApp . Vedere ["NetApp Active IQ"](#) per maggiori informazioni.

Cosa sono gli eventi del sistema di gestione degli eventi

L'Event Management System (EMS) raccoglie i dati degli eventi da diverse parti del kernel ONTAP e fornisce meccanismi di inoltro degli eventi. Questi eventi ONTAP possono essere segnalati come eventi EMS in Unified Manager. Il monitoraggio e la gestione centralizzati semplificano la configurazione degli eventi EMS critici e le notifiche di avviso basate su tali eventi EMS.

L'indirizzo 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 un evento nel cluster.

Esistono due metodi per ricevere eventi EMS in Unified Manager:

- Un certo numero di eventi EMS importanti vengono segnalati 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 l'evento è stato generato:

Funzionalità	Messaggi EMS automatici	Messaggi EMS sottoscritti
Eventi EMS disponibili	Sottoinsieme di eventi EMS	Tutti gli eventi EMS
Nome del messaggio EMS quando attivato	Nome evento Unified Manager (convertito dal nome evento EMS)	Non specifico nel formato "Errore EMS ricevuto". Il messaggio dettagliato fornisce il formato di notazione a punti dell'evento EMS effettivo
Messaggi ricevuti	Non appena il cluster sarà 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	Uguale agli altri eventi di Unified Manager: stati Nuovo, Riconosciuto, Risolto e Obsoleto	L'evento EMS diventa obsoleto dopo l'aggiornamento del cluster, ovvero dopo 15 minuti dalla creazione dell'evento.
Cattura gli eventi durante i tempi di inattività di Unified Manager	Sì, quando il sistema si avvia 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 "Stato dello spazio dei costituenti FlexGroup OK" indica che l'evento di errore "Problemi di spazio nei costituenti FlexGroup " è stato risolto. Gli eventi informativi non possono essere gestiti utilizzando lo stesso ciclo di vita degli altri tipi di gravità degli eventi; tuttavia, l'evento diventa automaticamente obsoleto se lo stesso volume riceve un altro evento di errore "Problemi di spazio".

Eventi EMS aggiunti automaticamente a Unified Manager

I seguenti eventi ONTAP EMS vengono aggiunti automaticamente a Unified Manager. Questi eventi verranno generati quando attivati su qualsiasi cluster monitorato da Unified Manager.

I seguenti eventi EMS sono disponibili durante il monitoraggio di cluster che eseguono il software ONTAP 9.5 o versioni successive:

Nome evento Unified Manager	Nome dell'evento EMS	Risorsa interessata	Gravità di Unified Manager
Accesso al livello cloud negato per la rilocalizzazione aggregata	arl.netra.ca.check.failed	Aggregato	Errore
Accesso al livello cloud negato per la rilocalizzazione dell'aggregato durante il failover dello storage	gb.netra.ca.check.failed	Aggregato	Errore
Risincronizzazione della replica mirror FabricPool completata	waf.ca.resync.complete	Grappolo	Errore
Spazio FabricPool quasi pieno	fabricpool.quasi.pieno	Grappolo	Errore
Periodo di grazia NVMe-oF iniziato	nvmf.graceperiod.start	Grappolo	Avvertimento
Periodo di grazia NVMe-oF attivo	nvmf.graceperiod.active	Grappolo	Avvertimento
Periodo di grazia NVMe-oF scaduto	nvmf.graceperiod.expired	Grappolo	Avvertimento
LUN distrutto	lun.distruggere	LUN	Informazioni
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	Nodo	Errore
Cloud AWS IAMCredsExpired	cloud.aws.iamCredsExpired	Nodo	Errore
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	Nodo	Errore
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	Nodo	Errore
Cloud AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	Nodo	Informazioni
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	Nodo	Errore

Nome evento Unified Manager	Nome dell'evento EMS	Risorsa interessata	Gravità di Unified Manager
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	Nodo	Errore
Cloud Tier Host non risolvibile	objstore.host.irrisolvibile	Nodo	Errore
Interfaccia di rete intercluster Cloud Tier inattiva	objstore.interclusterlifDown	Nodo	Errore
Richiesta di mancata corrispondenza della firma del livello cloud	osc.signatureMismatch	Nodo	Errore
Uno dei pool NFSv4 esaurito	Nblade.nfsV4PoolExhaust	Nodo	Critico
Memoria monitor QoS al massimo	qos.monitor.memory.maxed	Nodo	Errore
Memoria del monitor QoS ridotta	qos.monitor.memory.abba	Nodo	Informazioni
NVMeNS Destroy	NVMeNS.distruggi	Spazio dei nomi	Informazioni
NVMeNS Online	NVMeNS.offline	Spazio dei nomi	Informazioni
NVMeNS offline	NVMeNS.online	Spazio dei nomi	Informazioni
NVMeNS senza spazio	NVMeNS.spazio esaurito	Spazio dei nomi	Avvertimento
Replica sincrona fuori sincrono	sms.status.out.of.sync	Relazione SnapMirror	Avvertimento
Replica sincrona ripristinata	sms.status.in.sync	Relazione SnapMirror	Informazioni
Risincronizzazione automatica della replica sincrona non riuscita	tentativo di risincronizzazione sms fallito	Relazione SnapMirror	Errore
Molte connessioni CIFS	Nblade.cifsManyAuths	SVM	Errore

Nome evento Unified Manager	Nome dell'evento EMS	Risorsa interessata	Gravità di Unified Manager
Numero massimo di connessioni CIFS superato	Nblade.cifsMaxOpenSam eFile	SVM	Errore
Numero massimo di connessioni CIFS per utente superato	Nblade.cifsMaxSessPerU srConn	SVM	Errore
Conflitto di nomi NetBIOS CIFS	Nblade.cifsNbNameConfl ict	SVM	Errore
Tentativi di connettere una condivisione CIFS inesistente	Nblade.cifsNoPrivShare	SVM	Critico
Operazione di copia shadow CIFS non riuscita	cifs.shadowcopy.falliment o	SVM	Errore
Virus trovato dal server AV	Nblade.vscanVirusDetect ed	SVM	Errore
Nessuna connessione al server AV per la scansione virus	Nblade.vscanNoScanner Conn	SVM	Critico
Nessun server AV registrato	Nblade.vscanNoRegdSca nner	SVM	Errore
Nessuna connessione al server AV reattivo	Nblade.vscanConnInattivo	SVM	Informazioni
Il server AV è troppo occupato per accettare una nuova richiesta di scansione	Nblade.vscanConnBackPr essure	SVM	Errore
Tentativo di accesso non autorizzato al server AV	Nblade.vscanBadUserPriv Access	SVM	Errore
I componenti FlexGroup hanno problemi di spazio	i costituenti del gruppo flessibile hanno problemi di spazio	Volume	Errore
Costituenti FlexGroup Spazio Stato Tutto OK	flexgroup.constituents.spa ce.status.all.ok	Volume	Informazioni

Nome evento Unified Manager	Nome dell'evento EMS	Risorsa interessata	Gravità di Unified Manager
I componenti FlexGroup hanno problemi con gli inode	i costituenti del gruppo flessibile hanno problemi con gli inodi	Volume	Errore
Costituenti FlexGroup Inode Stato Tutto OK	flexgroup.constituents.inodes.status.all.ok	Volume	Informazioni
Spazio logico del volume quasi pieno	monitor.vol.nearFull.inc.save	Volume	Avvertimento
Volume Spazio Logico Pieno	monitor.vol.full.inc.save	Volume	Errore
Volume Spazio Logico Normale	monitor.vol.one.ok.inc.save	Volume	Informazioni
Errore di ridimensionamento automatico del volume WAFL	wafl.vol.autoSize.fail	Volume	Errore
WAFL Volume AutoSize Fatto	wafl.vol.autoSize.done	Volume	Informazioni
Timeout dell'operazione file WAFL REaddir	wafl.readdir.expired	Volume	Errore

Iscriviti agli eventi ONTAP EMS

È possibile abbonarsi per ricevere gli eventi EMS (Event Management System) generati dai sistemi installati con il software ONTAP . Un sottoinsieme di eventi EMS viene segnalato automaticamente a Unified Manager, ma gli eventi EMS aggiuntivi vengono segnalati solo se si è sottoscritti tali eventi.

Prima di iniziare

Non iscriverti agli eventi EMS che sono già stati aggiunti automaticamente a Unified Manager, poiché ciò potrebbe causare confusione quando si ricevono due eventi per lo stesso problema.

Puoi iscriverti a tutti gli eventi EMS che vuoi. Tutti gli eventi a cui ti iscrivi vengono convalidati e solo gli eventi convalidati vengono applicati ai cluster che stai monitorando 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* nella pagina Documentazione prodotto ONTAP 9 per un elenco degli eventi applicabili.

["Libreria prodotti ONTAP 9"](#)

È possibile configurare avvisi per gli eventi ONTAP EMS a cui ci si iscrive e creare script personalizzati da

eseguire per tali eventi.



Se non ricevi gli eventi ONTAP EMS a cui ti sei abbonato, potrebbe esserci un problema con la configurazione DNS del cluster che impedisce al cluster di raggiungere il server Unified Manager. Per risolvere questo problema, l'amministratore del cluster deve correggere la configurazione DNS del cluster e quindi riavviare Unified Manager. In questo modo gli eventi EMS in sospenso verranno trasferiti al server Unified Manager.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione evento**.
2. Nella pagina Configurazione evento, fare clic sul pulsante **Iscriviti agli eventi EMS**.
3. Nella finestra di dialogo Iscriviti agli eventi EMS, immettere il nome dell'evento ONTAP EMS 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` comando (prima di ONTAP 9) o il `event catalog show` comando (ONTAP 9 o successivo).

["Come configurare e ricevere avvisi dall'abbonamento agli eventi ONTAP EMS in Active IQ Unified Manager"](#)

4. Fare clic su **Aggiungi**.

L'evento EMS viene aggiunto all'elenco degli eventi EMS sottoscritti, ma la colonna Applicabile al cluster visualizza lo stato "Sconosciuto" per l'evento EMS aggiunto.

5. Fare clic su **Salva e chiudi** per registrare l'abbonamento all'evento EMS con il cluster.
6. Fai clic di nuovo su **Iscriviti agli eventi EMS**.

Nella colonna Applicabile al cluster per l'evento EMS aggiunto viene visualizzato lo stato "Sì".

Se lo stato non è "Sì", controllare l'ortografia del nome dell'evento ONTAP EMS. Se il nome è stato immesso in modo errato, è necessario rimuovere l'evento errato e quindi aggiungerlo nuovamente.

Quando si verifica l'evento ONTAP EMS, l'evento viene visualizzato nella pagina Eventi. È possibile selezionare l'evento per visualizzare i dettagli sull'evento EMS nella pagina Dettagli evento. È anche possibile gestire lo svolgimento dell'evento o creare avvisi per l'evento.

Cosa succede quando viene ricevuto un evento

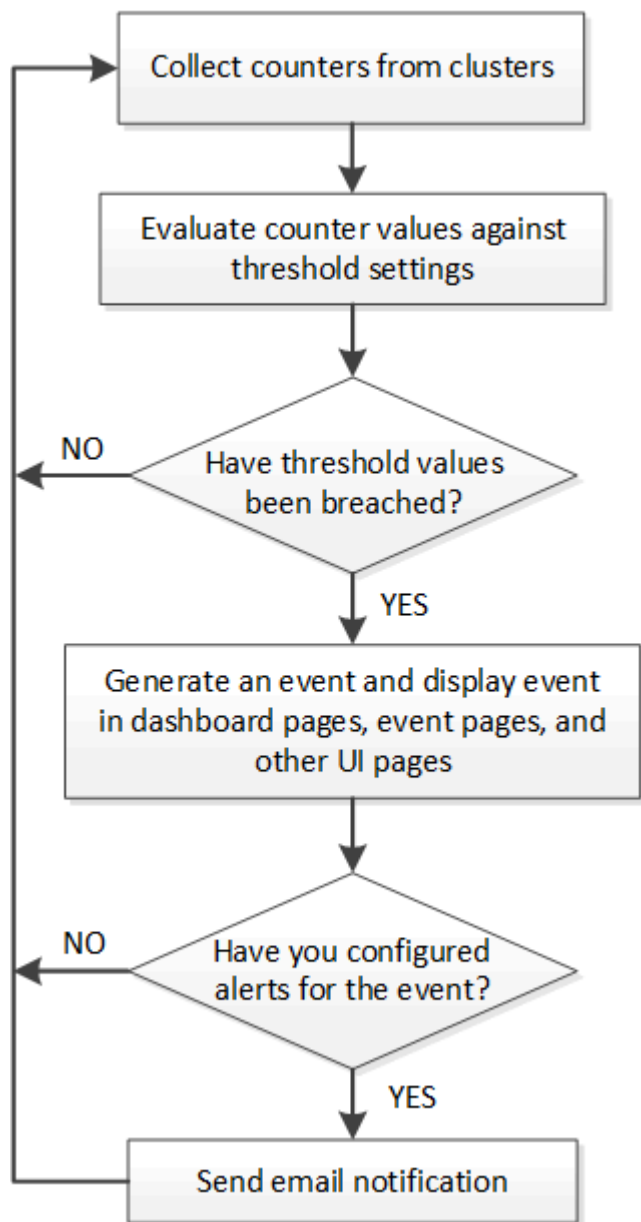
Quando Unified Manager riceve un evento, questo viene visualizzato nella pagina Dashboard, nella pagina Inventario Gestione eventi, nelle schede Riepilogo ed Esplora della pagina Cluster/Prestazioni e nella pagina Inventario specifica dell'oggetto (ad esempio, la pagina Inventario Volumi/Integrità).

Quando Unified Manager rileva più occorrenze continue della stessa condizione di evento per lo stesso componente del cluster, tratta tutte le occorrenze come un singolo evento, non come eventi separati. La durata dell'evento viene incrementata per indicare che l'evento è ancora attivo.

A seconda di come configuri le impostazioni nella pagina Impostazione avvisi, puoi avvisare altri utenti di questi eventi. L'avviso determina l'avvio delle seguenti azioni:

- È possibile inviare un'e-mail relativa all'evento a tutti gli utenti amministratori di Unified Manager.
- L'evento può essere inviato ad altri destinatari e-mail.
- 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.



Visualizza gli eventi e i dettagli dell'evento

È possibile visualizzare i dettagli di un evento attivato da Unified Manager per intraprendere azioni correttive. Ad esempio, se si verifica un evento sanitario Volume Offline, è possibile fare clic su tale evento per visualizzarne i dettagli ed eseguire azioni correttive.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

I dettagli dell'evento includono informazioni quali l'origine dell'evento, la causa dell'evento e qualsiasi nota correlata all'evento.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.

Per impostazione predefinita, la vista Tutti gli eventi attivi mostra gli eventi Nuovi e Riconosciuti (attivi) generati nei 7 giorni precedenti che hanno un Livello di impatto di Incidente o Rischio.

2. Se si desidera visualizzare una particolare categoria di eventi, ad esempio eventi di capacità o eventi di performance, fare clic su **Visualizza** e selezionare dal menu i tipi di evento.
3. Fare clic sul nome dell'evento di cui si desidera visualizzare i dettagli.

I dettagli dell'evento vengono visualizzati nella pagina Dettagli evento.

Visualizza eventi non assegnati

È possibile visualizzare gli eventi non assegnati e quindi assegnare ciascuno di essi a un utente in grado di risolverli.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.

Per impostazione predefinita, gli eventi Nuovi e Riconosciuti vengono visualizzati nella pagina dell'inventario Gestione eventi.

2. Dal riquadro **Filtri**, seleziona l'opzione di filtro **Non assegnato** nell'area **Assegnato a**.

Riconoscere e risolvere gli eventi

È opportuno riconoscere un evento prima di iniziare a lavorare sul problema che lo ha generato, in modo da non continuare a ricevere notifiche di avviso ripetute. Dopo aver adottato misure correttive per un evento specifico, dovresti contrassegnare l'evento come risolto.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile riconoscere e risolvere più eventi contemporaneamente.



Non è possibile riconoscere gli eventi informativi.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.
2. Dall'elenco degli eventi, eseguire le seguenti azioni per confermare gli eventi:

Se lo desidera...	Fai questo...
Riconosci e contrassegna un singolo evento come risolto	a. Fare clic sul nome dell'evento. b. Nella pagina Dettagli evento, determina la causa dell'evento. c. Fare clic su Riconosci. d. Adottare misure correttive appropriate. e. Fare clic su Segna come risolto.
Riconosci e contrassegna più eventi come risolti	a. Determinare la causa degli eventi dalla rispettiva pagina dei dettagli dell'evento. b. Seleziona gli eventi. c. Fare clic su Riconosci. d. Adottare le misure correttive appropriate. e. Fare clic su Segna come risolto.

Dopo che l'evento è stato contrassegnato come risolto, viene spostato nell'elenco degli eventi risolti.

3. **Facoltativo:** nell'area **Note e aggiornamenti**, aggiungi una nota su come hai affrontato l'evento, quindi fai clic su **Pubblica**.

Assegna eventi a utenti specifici

È possibile assegnare eventi non assegnati a se stessi o ad altri utenti, compresi 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 archiviazione, è possibile assegnare gli eventi per questi problemi all'utente che gestisce tale oggetto.

Prima di iniziare

- Il nome utente e l'ID e-mail devono essere configurati correttamente.
- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.
2. Nella pagina dell'inventario **Gestione eventi**, seleziona uno o più eventi che desideri assegnare.
3. Assegna l'evento scegliendo una delle seguenti opzioni:

Se vuoi assegnare l'evento a...	Allora fai così...
Te stesso	Fare clic su Assegna a > Io .

Se vuoi assegnare l'evento a...	Allora fai così...
Un altro utente	a. Fare clic su Assegna a > Un altro utente. b. Nella finestra di dialogo Assegna proprietario, immettere il nome utente oppure selezionare un utente dall'elenco a discesa. c. Fare clic su Assegna. All'utente viene inviata una notifica via e-mail.  Se non si immette un nome utente o non si seleziona un utente dall'elenco a discesa e si fa clic su Assegna, l'evento rimane non assegnato.

Disabilitare gli eventi indesiderati

Tutti gli eventi sono abilitati per impostazione predefinita. È possibile disabilitare gli eventi a livello globale per impedire la generazione di notifiche per eventi che non sono importanti nel proprio ambiente. È possibile abilitare gli eventi disabilitati quando si desidera riprendere a ricevere le relative notifiche.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Quando si disabilitano gli eventi, gli eventi generati in precedenza nel sistema vengono contrassegnati come obsoleti e gli avvisi configurati per tali eventi non vengono attivati. Quando si abilitano eventi disabilitati, le notifiche per questi eventi vengono generate a partire dal ciclo di monitoraggio successivo.

Quando si disabilita un evento per un oggetto (ad esempio, il vol offline evento) e in seguito si abilita l'evento, Unified Manager non genera nuovi eventi per gli oggetti che sono andati offline quando l'evento era nello stato disabilitato. Unified Manager genera un nuovo evento solo quando si verifica una modifica nello stato dell'oggetto dopo la riattivazione dell'evento.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione evento**.
2. Nella pagina **Impostazione evento**, disabilita o abilita gli eventi scegliendo una delle seguenti opzioni:

Se lo desidera...	Allora fai così...
Disabilitare gli eventi	a. Fare clic su Disabilita. b. Nella finestra di dialogo Disabilita eventi, seleziona la gravità dell'evento. c. Nella colonna Eventi corrispondenti, seleziona gli eventi che desideri disabilitare in base alla gravità dell'evento, quindi fai clic sulla freccia destra per spostare tali eventi nella colonna Disabilita eventi. d. Fare clic su Salva e chiudi. e. Verificare che gli eventi disabilitati siano visualizzati nella vista elenco della pagina Impostazione evento.
Abilita eventi	a. Seleziona la casella di controllo per l'evento o gli eventi che desideri abilitare. b. Fare clic su Abilita.

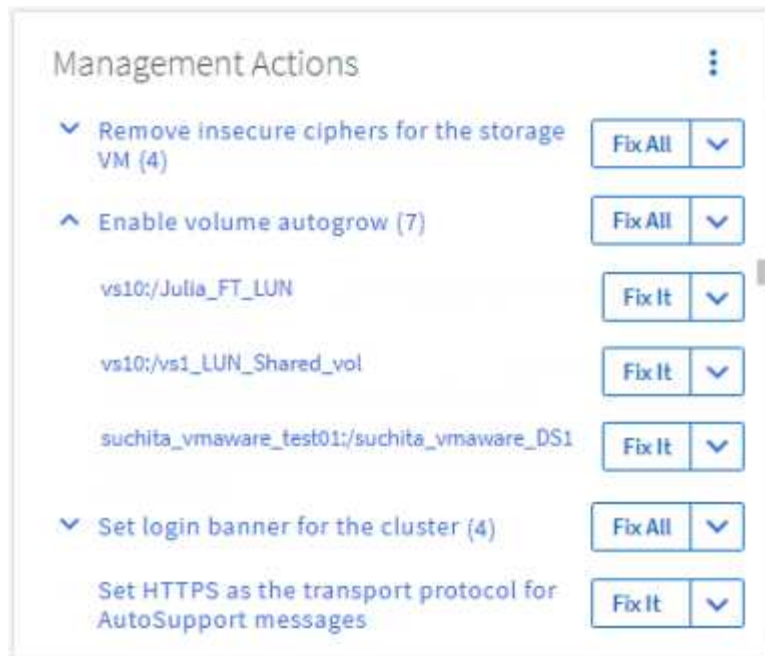
Risolvi i problemi utilizzando la correzione automatica di Unified Manager

Ci sono alcuni eventi che Unified Manager può diagnosticare in modo approfondito e fornire una soluzione univoca utilizzando il pulsante **Correggi**. Se disponibili, tali risoluzioni vengono visualizzate nella Dashboard, nella pagina dei dettagli dell'evento e nella selezione Analisi del carico di lavoro nel menu di navigazione a sinistra.

La maggior parte degli eventi ha diverse possibili risoluzioni, visualizzate nella pagina dei dettagli dell'evento, in modo da poter implementare la soluzione migliore utilizzando ONTAP System Manager o ONTAP CLI. Un'azione **Correggi** è disponibile quando Unified Manager ha stabilito che esiste un'unica soluzione per risolvere il problema e che può essere risolto utilizzando un comando ONTAP CLI.

Passi

1. Per visualizzare gli eventi che possono essere risolti dalla **Dashboard**, fare clic su **Dashboard**.



2. Per risolvere uno qualsiasi dei problemi che Unified Manager può risolvere, fare clic sul pulsante **Risolvi**. Per risolvere un problema che riguarda più oggetti, fare clic sul pulsante **Correggi tutto**.

Per informazioni sui problemi che possono essere risolti tramite la correzione automatica, vedere ["Quali problemi può risolvere Unified Manager"](#).

Abilita e disabilita la segnalazione degli eventi Active IQ

Per impostazione predefinita, gli eventi della piattaforma Active IQ vengono generati e visualizzati nell'interfaccia utente di Unified Manager. Se ritieni che questi eventi siano troppo "rumorosi" o che non desideri visualizzarli in Unified Manager, puoi disabilitarne la generazione. Se desideri riprendere a ricevere queste notifiche, puoi attivarle in un secondo momento.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Quando si disabilita questa funzionalità, Unified Manager smette immediatamente di ricevere gli eventi della piattaforma Active IQ.

Quando si abilita questa funzionalità, 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disattiva o attiva gli eventi della piattaforma Active IQ scegliendo una delle seguenti opzioni:

Se lo desidera...	Allora fai così...
Disabilita gli eventi della piattaforma Active IQ	Nel pannello *Eventi Active IQ *, spostare il cursore verso sinistra.
Abilita gli eventi della piattaforma Active IQ	Nel pannello *Eventi Active IQ *, spostare il cursore verso destra.

Carica un nuovo file di regole Active IQ

Unified Manager verifica automaticamente la presenza di nuovi file di eventi (regole) Active IQ e scarica un nuovo file quando sono presenti nuove regole. Tuttavia, nei siti senza accesso alla rete esterna, è necessario caricare manualmente il file delle regole.



Le regole Active IQ sono anche chiamate regole sicure Config Advisor (CA).

Quando si installa o si aggiorna Unified Manager a una versione 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 NetApp per assicurarsi che vengano generati eventi aggiornati e che i sistemi di storage continuino a funzionare in modo ottimale.

Prima di iniziare

- È necessario abilitare la segnalazione degli eventi del portale Active IQ . Questa funzione è abilitata per impostazione predefinita. Per informazioni, vedere "[Abilitazione degli eventi del portale Active IQ](#)".
- È necessario scaricare il file delle regole dal sito di supporto NetApp .

Il file delle regole si trova in: https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Passi

1. Su un computer con accesso alla rete, vai al sito di supporto NetApp e scarica le regole correnti .zip file.

Il pacchetto di regole in bundle include il repository delle 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 è incluso per impostazione predefinita nel programma di installazione. Puoi scaricare il file *secure_rules.zip* dal sito di supporto e caricarlo per visualizzare l'articolo della Knowledge Base per tutte le regole.

2. Trasferisci il file delle regole su un supporto che puoi portare nell'area protetta e poi copialo su un sistema nell'area protetta.
3. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione evento**.
4. Nella pagina **Impostazione evento**, fare clic sul pulsante **Carica regole**.
5. Nella finestra di dialogo **Regole di caricamento**, vai alle regole e seleziona .zip file scaricato e clicca su **Carica**.

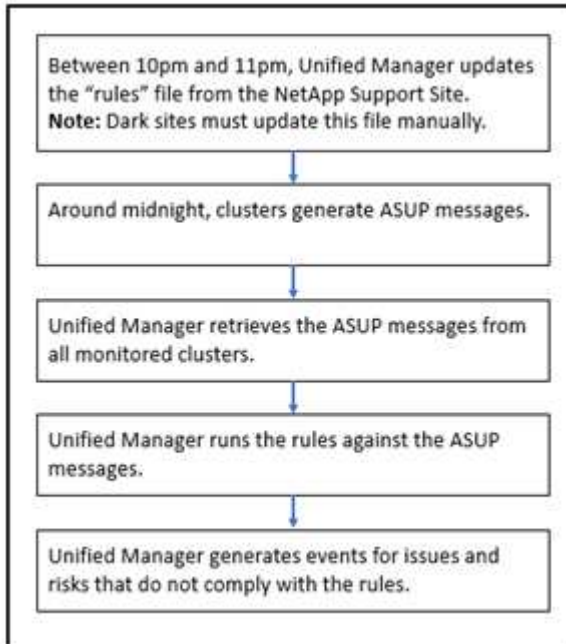
Questo processo può richiedere alcuni minuti.

Il file delle regole viene decompresso sul server Unified Manager. Dopo che i cluster gestiti generano un file AutoSupport dopo mezzanotte, Unified Manager verifica i cluster rispetto al file delle regole e genera nuovi eventi di rischio e incidente secondo necessità.

Per ulteriori informazioni, consultare questo articolo della Knowledge Base (KB): ["Come aggiornare manualmente le regole AIQCA Secure 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 Unified Manager come mostrato nel diagramma seguente.

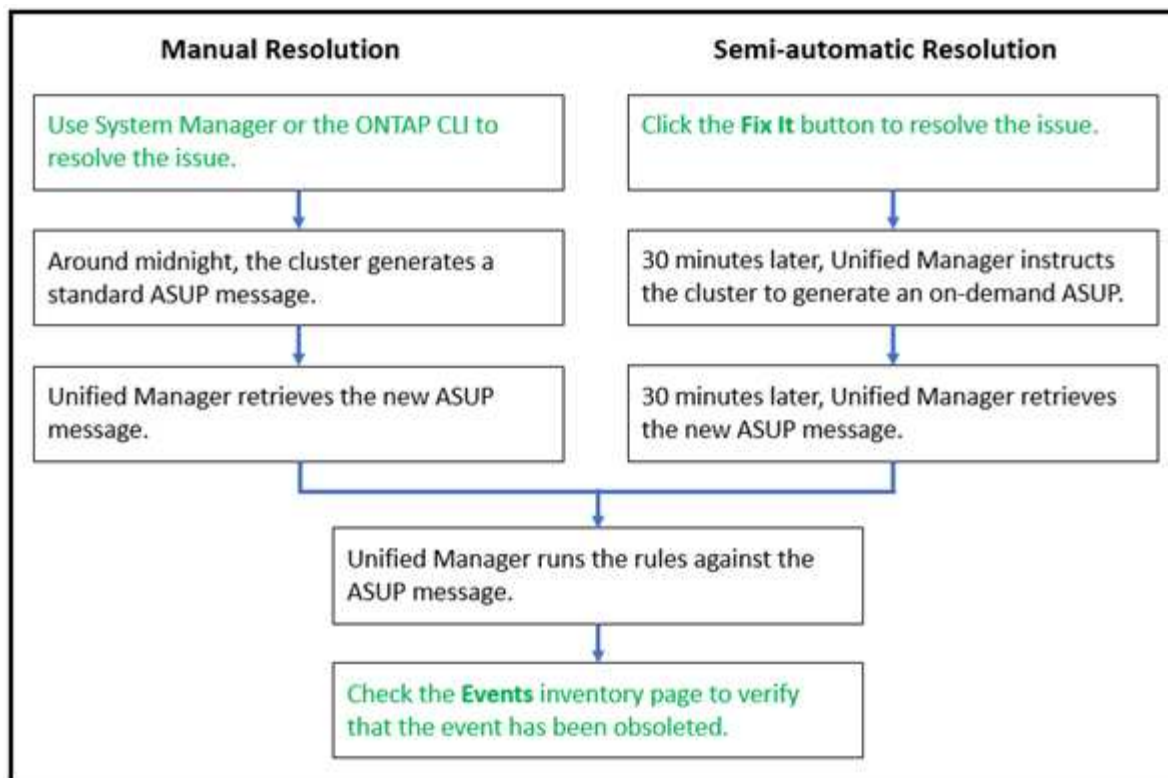


Come puoi vedere, il file delle regole compilato sulla piattaforma Active IQ viene mantenuto aggiornato, i messaggi AutoSupport del cluster vengono generati quotidianamente e Unified Manager aggiorna quotidianamente l'elenco degli eventi.

Risolvi gli eventi della piattaforma Active IQ

Gli incidenti e i rischi della piattaforma Active IQ sono simili ad altri eventi di Unified Manager perché possono essere assegnati ad altri utenti per la risoluzione e hanno gli stessi stati disponibili. Tuttavia, se risolvi questo tipo di eventi utilizzando il pulsante **Correggi**, puoi verificare la risoluzione entro poche ore.

Il diagramma seguente mostra le azioni che è necessario intraprendere (in verde) e l'azione intrapresa da Unified Manager (in nero) quando si risolvono gli eventi generati dalla piattaforma Active IQ .



Quando si esegue una risoluzione manuale, è necessario accedere a System Manager o all'interfaccia della riga di comando ONTAP per risolvere il problema. Sarà possibile verificare il problema solo dopo che il cluster avrà generato un nuovo messaggio AutoSupport a mezzanotte.

Eseguendo una risoluzione semiautomatica tramite il pulsante **Correggi** è possibile verificare che la correzione sia avvenuta correttamente entro poche ore.

Configurare le impostazioni di conservazione degli eventi

È possibile specificare il numero di mesi per cui un evento viene conservato nel server Unified Manager prima di essere eliminato automaticamente.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Conservare gli eventi per più di 6 mesi potrebbe influire sulle prestazioni del server e non è consigliato.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Conservazione dati**.
2. Nella pagina **Conservazione dati**, seleziona il cursore nell'area Conservazione eventi e spostalo sul numero di mesi per cui gli eventi devono essere conservati, quindi fai clic su **Salva**.

Cos'è una finestra di manutenzione di Unified Manager

È possibile definire una finestra di manutenzione di Unified Manager per sopprimere eventi e avvisi per un intervallo di tempo specifico quando è stata pianificata la manutenzione del cluster e non si desidera ricevere un'ondata di notifiche indesiderate.

All'avvio della finestra di manutenzione, nella pagina dell'inventario di Gestione eventi viene pubblicato l'evento "Finestra di manutenzione oggetto avviata". Questo evento diventa automaticamente obsoleto al termine della finestra di manutenzione.

Durante una finestra di manutenzione, gli eventi relativi a tutti gli oggetti su quel cluster vengono comunque generati, ma non vengono visualizzati in nessuna pagina dell'interfaccia utente e non vengono inviati avvisi o altri tipi di notifiche per questi eventi. Tuttavia, è possibile visualizzare gli eventi generati per tutti gli oggetti di archiviazione durante una finestra di manutenzione selezionando una delle opzioni Visualizza nella pagina Inventario Gestione eventi.

È possibile pianificare l'avvio di una finestra di manutenzione in futuro, modificare gli orari di inizio e fine di una finestra di manutenzione pianificata e annullare una finestra di manutenzione pianificata.

Pianifica una finestra di manutenzione per disabilitare le notifiche degli eventi del cluster

Se è previsto un periodo di inattività per un cluster, ad esempio per aggiornare il cluster o spostare uno dei nodi, è possibile sopprimere gli eventi e gli avvisi che normalmente verrebbero generati durante tale intervallo di tempo pianificando una finestra di manutenzione di Unified Manager.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Durante una finestra di manutenzione, gli eventi relativi a tutti gli oggetti su quel cluster vengono comunque generati, ma non vengono visualizzati nella pagina degli eventi e non vengono inviati avvisi o altri tipi di notifiche per questi eventi.

L'orario immesso per la finestra di manutenzione si basa sull'orario del server Unified Manager.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.
2. Nella colonna **Modalità di manutenzione** del cluster, seleziona il pulsante del cursore e spostalo verso destra.

Viene visualizzata la finestra del calendario.

3. Selezionare la data e l'ora di inizio e fine della finestra di manutenzione e fare clic su **Applica**.

Accanto al pulsante del cursore viene visualizzato il messaggio "Programmato".

Una volta raggiunta l'ora di inizio, il cluster entra in modalità di manutenzione e viene generato un evento "Finestra di manutenzione oggetto avviata".

Modificare o annullare una finestra di manutenzione programmata

Se hai configurato una finestra di manutenzione di Unified Manager che si verificherà in futuro, puoi modificare gli orari di inizio e fine oppure annullare la finestra di manutenzione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

L'annullamento di una finestra di manutenzione in esecuzione è utile se è stata completata la manutenzione del cluster prima dell'orario di fine della finestra di manutenzione programmata e si desidera iniziare nuovamente a ricevere eventi e avvisi dal cluster.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione cluster**.
2. Nella colonna **Modalità di manutenzione** del cluster:

Se lo desidera...	Esegui questo passaggio...
Modificare l'intervallo di tempo per una finestra di manutenzione programmata	a. Fare clic sul testo "Programmato" accanto al pulsante del cursore. b. Modifica la data e l'ora di inizio e/o fine e fai clic su Applica.
Estendere la durata di una finestra di manutenzione attiva	a. Fare clic sul testo "Attivo" accanto al pulsante del cursore. b. Modifica la data e l'ora di fine e fai clic su Applica.
Annullare una finestra di manutenzione programmata	Selezionare il pulsante del cursore e spostarlo verso sinistra.
Annulla una finestra di manutenzione attiva	Selezionare il pulsante del cursore e spostarlo verso sinistra.

Visualizza gli eventi che si sono verificati durante una finestra di manutenzione

Se necessario, è possibile visualizzare gli eventi generati per tutti gli oggetti di archiviazione durante una finestra di manutenzione di Unified Manager. La maggior parte degli eventi apparirà nello stato Obsoleto una volta completata la finestra di manutenzione e quando tutte le risorse di sistema saranno di nuovo operative.

Prima di iniziare

È necessario che sia stata completata almeno una finestra di manutenzione prima che qualsiasi evento sia disponibile.

Per impostazione predefinita, gli eventi verificatisi durante una finestra di manutenzione non vengono visualizzati nella pagina dell'inventario di Gestione eventi.

Passi

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 dell'inventario Gestione eventi.

2. Dal riquadro Visualizza, seleziona l'opzione **Tutti gli eventi generati durante la manutenzione**.

Viene visualizzato l'elenco degli eventi attivati negli ultimi 7 giorni da tutte le sessioni della finestra di

manutenzione e da tutti i cluster.

3. Se sono state attivate più finestre di manutenzione per un singolo cluster, è possibile 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.

Gestire gli 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 quali la mancanza di spazio disponibile su disco o la mancanza di memoria sul sistema host possono attivare eventi della stazione di gestione che vengono visualizzati come messaggi banner nella parte superiore dell'interfaccia utente.

Gli eventi della stazione di gestione indicano un problema con il sistema host su cui è installato Unified Manager. Esempi di problemi della stazione di gestione includono lo spazio su disco insufficiente sul sistema host, la mancanza di un ciclo regolare di raccolta dati da parte di Unified Manager e il mancato completamento, o il completamento tardivo, dell'analisi delle statistiche perché è stato avviato il successivo poll di 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 nei messaggi banner.

Fare un passo

1. Per visualizzare le informazioni sugli eventi della stazione di gestione, eseguire le seguenti azioni:

Se lo desidera...	Fai questo...
Visualizza i dettagli dell'evento	Fare clic sul banner dell'evento per visualizzare la pagina dei dettagli dell'evento, che include le soluzioni suggerite per il problema.
Visualizza tutti gli eventi della stazione di gestione	a. Nel riquadro di navigazione a 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.

Scopri di più sugli eventi

Comprendere i concetti relativi agli eventi aiuta a gestire in modo efficiente i cluster e gli oggetti cluster e a definire gli avvisi in modo appropriato.

Definizioni dello stato dell'evento

Lo stato di un evento aiuta a stabilire se è necessaria un'azione correttiva appropriata. Un evento può essere Nuovo, Riconosciuto, Risolto o Obsoleto. Si noti che sia gli eventi Nuovi che quelli Riconosciuti sono considerati eventi attivi.

Gli stati dell'evento sono i seguenti:

- **Nuovo**

Lo stato di un nuovo evento.

- **Riconosciuto**

Lo stato di un evento quando lo hai riconosciuto.

- **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 diversi stati di un evento

Gli esempi seguenti illustrano le modifiche di stato degli eventi manuali e automatici.

Quando viene attivato l'evento Cluster non raggiungibile, lo stato dell'evento è Nuovo. Quando si riconosce l'evento, lo stato dell'evento cambia in Riconosciuto. Dopo aver adottato un'azione correttiva appropriata, è necessario contrassegnare l'evento come risolto. Lo stato dell'evento cambia quindi in Risolto.

Se l'evento Cluster non raggiungibile viene generato a causa di un'interruzione di corrente, quando l'alimentazione viene ripristinata il cluster inizia a funzionare senza alcun intervento dell'amministratore. Pertanto, l'evento Cluster non raggiungibile non è più valido e lo stato dell'evento cambia in Obsoleto nel ciclo di monitoraggio successivo.

Unified Manager invia un avviso quando un evento è nello stato Obsoleto o Risolto. L'oggetto e il contenuto dell'e-mail di un avviso forniscono informazioni sullo stato dell'evento. Una trap SNMP include anche informazioni sullo stato dell'evento.

Descrizione dei tipi di gravità degli eventi

A ciascun evento è associato un tipo di gravità per aiutarti a stabilire la priorità degli eventi che richiedono un'azione correttiva immediata.

- **Critico**

Si è verificato un problema che potrebbe causare l'interruzione del servizio se non si interviene immediatamente con misure correttive.

Gli eventi critici per le prestazioni vengono inviati solo da soglie definite dall'utente.

- **Errore**

L'origine dell'evento è ancora funzionante; tuttavia, è necessario un intervento correttivo per evitare l'interruzione del servizio.

- **Avvertimento**

Si è verificato un evento di cui dovresti essere a conoscenza nell'origine dell'evento oppure un contatore delle prestazioni per un oggetto cluster è fuori dall'intervallo normale e deve essere monitorato per assicurarti che non raggiunga la gravità critica. Eventi di questa gravità non causano interruzioni del servizio e potrebbero non essere necessarie misure correttive immediate.

Gli eventi di avviso sulle prestazioni vengono inviati da soglie definite dall'utente, definite dal sistema o dinamiche.

- **Informazioni**

L'evento si verifica quando viene scoperto un nuovo oggetto o quando viene eseguita un'azione da parte dell'utente. Ad esempio, quando viene eliminato un oggetto di archiviazione o quando si verificano modifiche alla configurazione, viene generato l'evento con tipo di gravità Informazioni.

Gli eventi informativi vengono inviati direttamente da ONTAP quando rileva una modifica alla configurazione.

Descrizione dei livelli di impatto dell'evento

A ciascun evento è associato un livello di impatto (incidente, rischio, evento o aggiornamento) per aiutarti a stabilire 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 di 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 pari a Incidente sono i più gravi. È necessario adottare misure correttive immediate per evitare interruzioni del servizio.

- **Rischio**

Un rischio è un insieme di eventi che possono potenzialmente causare l'interruzione della fornitura di 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 pari a Rischio possono causare l'interruzione del servizio. Potrebbero essere necessarie misure correttive.

- **Evento**

Un evento è uno stato o una modifica dello stato degli oggetti di archiviazione e dei loro attributi. Gli eventi con un livello di impatto Evento sono informativi e non richiedono azioni correttive.

- **Aggiornamento**

Gli eventi di aggiornamento sono un tipo specifico di evento segnalato dalla piattaforma Active IQ. Questi eventi identificano problemi per la cui risoluzione è necessario aggiornare il software ONTAP, il firmware del nodo o il software del sistema operativo (per gli avvisi di sicurezza). Per alcuni di questi problemi potrebbe essere necessario intervenire immediatamente, mentre per altri potrebbe essere necessario attendere la successiva manutenzione programmata.

Descrizione delle aree di impatto dell'evento

Gli eventi sono classificati in sei aree di impatto (disponibilità, capacità, configurazione,

prestazioni, protezione e sicurezza) per consentirti di concentrarti sui tipi di eventi di cui sei responsabile.

- **Disponibilità**

Gli eventi di disponibilità ti avvisano se un oggetto di archiviazione va offline, se un servizio di protocollo si interrompe, se si verifica un problema con il failover dell'archiviazione o se si verifica un problema con l'hardware.

- **Capacità**

Gli eventi di capacità ti avvisano se i tuoi aggregati, volumi, LUN o namespace si stanno avvicinando o hanno raggiunto una soglia di dimensione oppure se il tasso di crescita è insolito per il tuo ambiente.

- **Configurazione**

Gli eventi di configurazione informano l'utente sulla scoperta, l'eliminazione, l'aggiunta, la rimozione o la ridenominazione degli oggetti di archiviazione. Gli eventi di configurazione hanno un livello di impatto Evento e un tipo di gravità Informazione.

- **Prestazione**

Gli eventi di prestazione ti informano sulle condizioni delle risorse, della configurazione o delle attività sul tuo cluster che potrebbero influire negativamente sulla velocità di input o recupero dell'archiviazione dei dati sugli oggetti di archiviazione monitorati.

- **Protezione**

Gli eventi di protezione ti avvisano di incidenti o rischi che coinvolgono le 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 vengono categorizzati nell'area di impatto della protezione.

- **Sicurezza**

Gli eventi di sicurezza ti informano sul livello di sicurezza dei tuoi cluster ONTAP , delle macchine virtuali di archiviazione (SVM) e dei volumi in base ai parametri definiti in ["Guida al rafforzamento della sicurezza NetApp per ONTAP 9"](#) .

Inoltre, quest'area include gli eventi di aggiornamento segnalati dalla piattaforma Active IQ .

Come viene calcolato lo stato dell'oggetto

Lo stato dell'oggetto è determinato dall'evento più grave che attualmente presenta uno stato Nuovo o Riconosciuto. Ad esempio, se lo stato di un oggetto è Errore, uno degli eventi dell'oggetto ha un tipo di gravità Errore. Una volta intrapresa l'azione correttiva, lo stato dell'evento passa a Risolto.

Dettagli del grafico degli eventi di prestazioni dinamiche

Per gli eventi di prestazioni dinamiche, la sezione Diagnosi di sistema della pagina Dettagli evento elenca i carichi di lavoro principali con la latenza o l'utilizzo più elevati del componente cluster in competizione.

Le statistiche sulle prestazioni si basano sul momento in cui l'evento prestazionale è stato rilevato fino all'ultima analisi dell'evento. I grafici mostrano anche le statistiche storiche delle prestazioni del componente del cluster in competizione.

Ad esempio, è possibile identificare i carichi di lavoro con un elevato utilizzo di un componente per determinare quale carico di lavoro spostare su un componente meno utilizzato. Spostando il carico di lavoro si ridurrebbe la quantità di lavoro sul componente corrente, eventualmente eliminando il componente dalla competizione. Nella parte superiore di questa sezione sono riportati l'intervallo di data e ora in cui un evento è stato rilevato e analizzato l'ultima volta. Per gli eventi attivi (nuovi o riconosciuti), viene aggiornato l'ultimo orario analizzato.

I grafici di latenza e attività mostrano i nomi dei carichi di lavoro principali quando si passa 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, inclusi *squali*, *bulli* o *vittime*, e vengono visualizzati i dettagli sulla loro latenza e sul loro utilizzo sul componente del cluster in competizione. È possibile confrontare il valore effettivo con quello previsto per vedere quando il carico di lavoro si è trovato al di fuori dell'intervallo previsto di latenza o utilizzo. Per informazioni, vedere ["Tipi di carichi di lavoro monitorati da Unified Manager"](#).



Quando si ordina in base alla deviazione massima della 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 prestazioni dinamiche, vedere ["Analisi degli eventi dalle soglie di prestazioni dinamiche"](#).

Per informazioni su come Unified Manager classifica i carichi di lavoro e determina l'ordine di ordinamento, vedere ["Come Unified Manager determina l'impatto sulle prestazioni di un evento"](#).

I dati nei grafici mostrano le statistiche delle prestazioni delle 24 ore precedenti l'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 che l'evento è stato rilevato, quindi le sue 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 massima (massima) della latenza.



Poiché Unified Manager conserva un massimo di 30 giorni di dati storici di 5 minuti sulle prestazioni e sugli eventi, se l'evento ha più di 30 giorni, non vengono visualizzati dati sulle prestazioni.

- **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 componenti**

Visualizza i dettagli sull'utilizzo del carico di lavoro del componente del cluster in competizione. Nei grafici, l'utilizzo effettivo è rappresentato dalla linea blu. Una barra rossa evidenzia la durata dell'evento, dal momento del rilevamento all'ultimo momento analizzato. Per maggiori informazioni, vedere ["Valori di misurazione delle prestazioni del carico di lavoro"](#).



Per il componente di rete, poiché le statistiche sulle prestazioni di rete provengono dall'attività esterna al cluster, questa colonna non viene visualizzata.

- **Utilizzo dei componenti**

Visualizza la cronologia di utilizzo, in percentuale, per i componenti di elaborazione di rete, elaborazione dati e aggregazione oppure la cronologia dell'attività, in percentuale, per il componente del gruppo di policy 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.

- **Cronologia totale MB/s scritti**

Solo per il componente Risorse MetroCluster, mostra la velocità effettiva di scrittura totale, in megabyte al secondo (MBps), per tutti i carichi di lavoro del volume sottoposti a mirroring sul cluster partner in una configurazione MetroCluster.

- **Cronologia eventi**

Visualizza linee ombreggiate in rosso per indicare gli eventi storici per il componente in questione. Per gli eventi obsoleti, il grafico mostra gli eventi che si sono verificati prima che l'evento selezionato venisse rilevato e dopo che è stato risolto.

Modifiche alla configurazione rilevate da Unified Manager

Unified Manager monitora i cluster per rilevare eventuali modifiche alla configurazione, aiutandoti a stabilire se una modifica potrebbe aver causato o contribuito a un evento di prestazioni. Le pagine di Performance Explorer visualizzano un'icona di evento di modifica (●) 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 avuto un impatto sulle prestazioni dell'oggetto cluster selezionato. Se la modifica è stata rilevata contemporaneamente o più o meno nello stesso momento di un evento di prestazione, la modifica potrebbe aver contribuito al problema, causando l'attivazione dell'avviso di evento.

Unified Manager può rilevare i seguenti eventi di modifica, classificati come eventi informativi:

- Un volume si sposta tra aggregati.

Unified Manager è in grado di rilevare quando lo spostamento è in corso, completato o fallito. Se Unified Manager è inattivo durante lo spostamento di un volume, quando torna attivo 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 uno o più carichi di lavoro monitorati cambia.

La modifica del limite di un gruppo di policy può causare picchi intermittenti nella latenza (tempo di risposta), che potrebbero anche attivare eventi per il gruppo di policy. La latenza torna gradualmente alla normalità e tutti gli eventi causati dai picchi diventano obsoleti.

- Un nodo in una coppia HA prende il controllo o restituisce lo storage al nodo partner.

Unified Manager è in grado di rilevare quando l'operazione di acquisizione, acquisizione parziale o restituzione è stata completata. Se l'acquisizione è causata da un nodo in panico, Unified Manager non rileva l'evento.

- Un'operazione di aggiornamento o ripristino ONTAP è stata completata correttamente.

Vengono visualizzate la versione precedente e quella nuova.

Elenco degli eventi e dei tipi di gravità

È possibile utilizzare l'elenco degli eventi per acquisire maggiore familiarità con le categorie degli eventi, i nomi degli eventi e il tipo di gravità di ciascun evento che potrebbe essere visualizzato in Unified Manager. Gli eventi sono elencati in ordine alfabetico per categoria di oggetto.

Eventi aggregati

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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Aggregato offline (ocumEvtAggregateState Offline)	Incidente	Aggregato	Critico
Aggregato non riuscito (ocumEvtAggregateState Failed)	Incidente	Aggregato	Critico
Aggregato limitato (ocumEvtAggregateState Restricted)	Rischio	Aggregato	Avvertimento
Ricostruzione aggregata (ocumEvtAggregateRaidStateReconstructing)	Rischio	Aggregato	Avvertimento
Aggregato degradato (ocumEvtAggregateRaidStateDegraded)	Rischio	Aggregato	Avvertimento

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Livello cloud parzialmente raggiungibile (ocumEventCloudTierPartiallyReachable)	Rischio	Aggregato	Avvertimento
Livello cloud non raggiungibile (ocumEventCloudTierUnreachable)	Rischio	Aggregato	Errore
Accesso al livello cloud negato per la rilocazione dell'aggregato (arINetraCaCheckFailed)	Rischio	Aggregato	Errore
Accesso al livello cloud negato per la rilocazione dell'aggregato durante il failover dell'archiviazione (gbNetraCaCheckFailed)	Rischio	Aggregato	Errore
Aggregato MetroCluster lasciato indietro (ocumEvtMetroClusterAggregateLeftBehind)	Rischio	Aggregato	Errore
Mirroring aggregato MetroCluster degradato (ocumEvtMetroClusterAggregateMirrorDegraded)	Rischio	Aggregato	Errore

Area di impatto: capacità

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Spazio aggregato quasi pieno (ocumEvtAggregateNearlyFull)	Rischio	Aggregato	Avvertimento
Spazio aggregato pieno (ocumEvtAggregateFull)	Rischio	Aggregato	Errore

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Giorni aggregati fino al riempimento (ocumEvtAggregateDaysUntilFullSoon)	Rischio	Aggregato	Errore
Aggregato sovracompresso (ocumEvtAggregateOvercommitted)	Rischio	Aggregato	Errore
Aggregato quasi sovracompresso (ocumEvtAggregateAlmostOvercommitted)	Rischio	Aggregato	Avvertimento
Riserva snapshot aggregata completa (ocumEvtAggregateSnapshotReserveFull)	Rischio	Aggregato	Avvertimento
Tasso di crescita aggregato anomalo (ocumEvtAggregateGrowthRateAbnormal)	Rischio	Aggregato	Avvertimento

Area di impatto: configurazione

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Aggregato scoperto (non applicabile)	Evento	Aggregato	Informazioni
Aggregato rinominato (non applicabile)	Evento	Aggregato	Informazioni
Aggregato eliminato (non applicabile)	Evento	Nodo	Informazioni

Area di impatto: prestazioni

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica IOPS aggregata violata (ocumAggregateIopsIncident)	Incidente	Aggregato	Critico
Soglia di avviso IOPS aggregati violata (ocumAggregateIopsWarning)	Rischio	Aggregato	Avvertimento
Soglia critica aggregata MB/s violata (ocumAggregateMbpsIncident)	Incidente	Aggregato	Critico
Soglia di avviso MB/s aggregato violata (ocumAggregateMbpsWarning)	Rischio	Aggregato	Avvertimento
Soglia critica di latenza aggregata violata (ocumAggregateLatencyIncident)	Incidente	Aggregato	Critico
Soglia di avviso di latenza aggregata violata (ocumAggregateLatencyWarning)	Rischio	Aggregato	Avvertimento
Capacità di prestazioni aggregate utilizzata soglia critica violata (ocumAggregatePerfCapacityUsedIncident)	Incidente	Aggregato	Critico
Soglia di avviso per la capacità di prestazioni aggregate utilizzata superata (ocumAggregatePerfCapacityUsedWarning)	Rischio	Aggregato	Avvertimento
Soglia critica di utilizzo aggregato violata (ocumAggregateUtilizationIncident)	Incidente	Aggregato	Critico

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia di avviso di utilizzo aggregato superata (ocumAggregateUtilizationWarning)	Rischio	Aggregato	Avvertimento
Superata la soglia di utilizzo eccessivo dei dischi aggregati (ocumAggregateDisksOverUtilizedWarning)	Rischio	Aggregato	Avvertimento
Soglia dinamica aggregata violata (ocumAggregateDynamicEventWarning)	Rischio	Aggregato	Avvertimento

Eventi di cluster

Gli eventi dei cluster forniscono informazioni sullo stato dei cluster, consentendo di monitorarli per individuare potenziali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento, il nome della trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Il cluster non ha dischi di riserva (ocumEvtDisksNoSpares)	Rischio	Grappolo	Avvertimento
Cluster non raggiungibile (ocumEvtClusterUnreachable)	Rischio	Grappolo	Errore
Monitoraggio del cluster non riuscito (ocumEvtClusterMonitoringFailed)	Rischio	Grappolo	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Limiti di capacità della licenza Cluster FabricPool violati (ocumEvtExternalCapacityTierSpaceFull)	Rischio	Grappolo	Avvertimento
Periodo di grazia NVMe-oF avviato *(nvmfGracePeriodStart)	Rischio	Grappolo	Avvertimento
Periodo di grazia NVMe-oF attivo *(nvmfGracePeriodActive)	Rischio	Grappolo	Avvertimento
Periodo di grazia NVMe-oF scaduto *(nvmfGracePeriodExpired)	Rischio	Grappolo	Avvertimento
Finestra di manutenzione dell'oggetto avviata (objectMaintenanceWindowStarted)	Evento	Grappolo	Critico
Finestra di manutenzione dell'oggetto terminata (objectMaintenanceWindowEnded)	Evento	Grappolo	Informazioni
Dischi di riserva MetroCluster lasciati indietro (ocumEvtSpareDiskLeftBehind)	Rischio	Grappolo	Errore
Commutazione automatica non pianificata MetroCluster disabilitata (ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Rischio	Grappolo	Avvertimento
Password utente del cluster modificata *(cluster.passwd.changed)	Evento	Grappolo	Informazioni

Area di impatto: capacità

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia di squilibrio della capacità del cluster violata (ocumConformanceNodeImbalanceWarning)	Rischio	Grappolo	Avvertimento
Pianificazione dei livelli del cluster cloud (clusterCloudTierPlanningWarning)	Rischio	Grappolo	Avvertimento
Completata la risincronizzazione della replica mirror FabricPool (wafCaResyncComplete)	Evento	Grappolo	Avvertimento
Spazio FabricPool quasi pieno (fabricpoolNearlyFull)	Rischio	Grappolo	Errore

Area di impatto: configurazione

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Nodo aggiunto (non applicabile)	Evento	Grappolo	Informazioni
Nodo rimosso (non applicabile)	Evento	Grappolo	Informazioni
Cluster rimosso (non applicabile)	Evento	Grappolo	Informazioni
Aggiunta cluster non riuscita (non applicabile)	Evento	Grappolo	Errore
Nome del cluster modificato (non applicabile)	Evento	Grappolo	Informazioni
Ricevuto servizio di emergenza medica (non applicabile)	Evento	Grappolo	Critico

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
EMS critico ricevuto (non applicabile)	Evento	Grappolo	Critico
Avviso ricevuto dal servizio di emergenza medica (non applicabile)	Evento	Grappolo	Errore
Errore EMS ricevuto (non applicabile)	Evento	Grappolo	Avvertimento
Avviso ricevuto dal servizio di emergenza medica (non applicabile)	Evento	Grappolo	Avvertimento
Debug EMS ricevuto (non applicabile)	Evento	Grappolo	Avvertimento
Avviso ricevuto da EMS (non applicabile)	Evento	Grappolo	Avvertimento
Informazioni EMS ricevute (non applicabile)	Evento	Grappolo	Avvertimento

Gli eventi ONTAP EMS sono classificati in tre livelli di gravità degli eventi Unified Manager.

Livello di gravità dell'evento Unified Manager	Livello di gravità dell'evento ONTAP EMS
Critico	Emergenza Critico
Errore	Attenzione
Avvertimento	Errore Avvertimento Debug Avviso Informativo

Area di impatto: prestazioni

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia di squilibrio del carico del cluster violata()	Rischio	Grappolo	Avvertimento
Soglia critica IOPS del cluster violata (ocumClusterIopsIncident)	Incidente	Grappolo	Critico
Soglia di avviso IOPS del cluster violata (ocumClusterIopsWarning)	Rischio	Grappolo	Avvertimento
Soglia critica MB/s del cluster violata (ocumClusterMbpsIncident)	Incidente	Grappolo	Critico
Soglia di avviso MB/s del cluster violata (ocumClusterMbpsWarning)	Rischio	Grappolo	Avvertimento
Soglia dinamica del cluster violata (ocumClusterDynamicEventWarning)	Rischio	Grappolo	Avvertimento

Area di impatto: sicurezza

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
AutoSupport del trasporto HTTPS disabilitato (ocumClusterASUPHttpsConfiguredDisabled)	Rischio	Grappolo	Avvertimento
Inoltro del registro non crittografato (ocumClusterAuditLogUnencrypted)	Rischio	Grappolo	Avvertimento
Utente amministratore locale predefinito abilitato (ocumClusterDefaultAdminEnabled)	Rischio	Grappolo	Avvertimento

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Modalità FIPS disabilitata (ocumClusterFipsDisabled)	Rischio	Grappolo	Avvertimento
Banner di accesso disabilitato (ocumClusterLoginBannerDisabled)	Rischio	Grappolo	Avvertimento
Banner di accesso modificato (ocumClusterLoginBannerChanged)	Rischio	Grappolo	Avvertimento
Destinazioni di inoltro dei log modificate (ocumLogForwardDestinationsChanged)	Rischio	Grappolo	Avvertimento
Nomi dei server NTP modificati (ocumNtpServerNamesChanged)	Rischio	Grappolo	Avvertimento
Il conteggio dei server NTP è basso (securityConfigNTPServerCountLowRisk)	Rischio	Grappolo	Avvertimento
Comunicazione peer del cluster non crittografata (ocumClusterPeerEncryptionDisabled)	Rischio	Grappolo	Avvertimento
SSH utilizza cifrari non sicuri (ocumClusterSSHInsecure)	Rischio	Grappolo	Avvertimento
Protocollo Telnet abilitato (ocumClusterTelnetEnabled)	Rischio	Grappolo	Avvertimento

Nome evento (nome trappola)	Livello di impatto	Tipo di fonte	Gravità
Le password di alcuni account utente ONTAP utilizzano la funzione hash MD5 meno sicura (ocumClusterMD5PasswordHashUsed)	Rischio	Grappolo	Avvertimento
Il cluster utilizza un certificato autofirmato (ocumClusterSelfSignedCertificate)	Rischio	Grappolo	Avvertimento
Cluster Remote Shell è abilitato (ocumClusterRshDisabled)	Rischio	Grappolo	Avvertimento
Certificato cluster in scadenza (ocumEvtClusterCertificateAboutToExpire)	Rischio	Grappolo	Avvertimento
Certificato cluster scaduto (ocumEvtClusterCertificateExpired)	Rischio	Grappolo	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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Dischi Flash - Blocchi di riserva quasi consumati (ocumEvtClusterFlashDiskFewerSpareBlockError)	Rischio	Grappolo	Errore
Dischi flash - Nessun blocco di riserva (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incidente	Grappolo	Critico

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Alcuni dischi non assegnati (ocumEvtClusterUnassignedDisksSome)	Rischio	Grappolo	Avvertimento
Alcuni dischi guasti (ocumEvtDisksSomeFailed)	Incidente	Grappolo	Critico

Eventi di recinti

Gli eventi degli enclosure forniscono informazioni sullo stato degli enclosure degli scaffali dei dischi nel data center, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Ventole del ripiano del disco guaste (ocumEvtShelfFanFailed)	Incidente	Scaffale portaoggetti	Critico
Alimentatori dello scaffale del disco guasti (ocumEvtShelfPowerSupplyFailed)	Incidente	Scaffale portaoggetti	Critico
Disk Shelf Multipath non configurato (ocumDiskShelfConnectivityNotInMultiPath)	Rischio	Nodo	Avvertimento
Questo evento non si applica a: - Cluster che si trovano in una configurazione MetroCluster - Le seguenti piattaforme: FAS2554, FAS2552, FAS2520 e FAS2240			

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Errore del percorso dello scaffale del disco (ocumDiskShelfConnectivityPathFailure)	Rischio	Scaffale portaoggetti	Avvertimento

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Ripiano del disco scoperto (non applicabile)	Evento	Nodo	Informazioni
Ripiani per dischi rimossi (non applicabile)	Evento	Nodo	Informazioni

Eventi per i fan

Gli eventi delle ventole forniscono informazioni sullo stato delle ventole sui 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Uno o più fan guasti (ocumEvtFansOneOrMoreFailed)	Incidente	Nodo	Critico

Eventi con flash card

Gli eventi delle schede flash forniscono informazioni sullo stato delle schede flash installate sui 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Schede didattiche 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: capacità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Inode quasi pieni (ocumEvtInodesAlmostFull)	Rischio	Volume	Avvertimento
Inode completi (ocumEvtInodesFull)	Rischio	Volume	Errore

Eventi dell'interfaccia di rete (LIF)

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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Stato dell'interfaccia di rete inattivo (ocumEvtLifStatusDown)	Rischio	Interfaccia	Errore
Stato dell'interfaccia di rete FC/FCoE inattivo (ocumEvtFCLifStatusDown)	Rischio	Interfaccia	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Failover dell'interfaccia di rete non possibile (ocumEvtLifFailoverNotPossible)	Rischio	Interfaccia	Avvertimento
Porta dell'interfaccia di rete non presente a casa (ocumEvtLifNotAtHomePort)	Rischio	Interfaccia	Avvertimento

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Percorso dell'interfaccia di rete non configurato (non applicabile)	Evento	Interfaccia	Informazioni

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica MB/s dell'interfaccia di rete violata (ocumNetworkLifMbpsIncident)	Incidente	Interfaccia	Critico
Soglia di avviso MB/s dell'interfaccia di rete violata (ocumNetworkLifMbpsWarning)	Rischio	Interfaccia	Avvertimento
Soglia critica MB/s dell'interfaccia di rete FC violata (ocumFcpLifMbpsIncident)	Incidente	Interfaccia	Critico
Soglia di avviso MB/s dell'interfaccia di rete FC violata (ocumFcpLifMbpsWarning)	Rischio	Interfaccia	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica MB/s dell'interfaccia di rete NVMf FC violata (ocumNvmfFcLifMbpsIncident)	Incidente	Interfaccia	Critico
Soglia di avviso MB/s dell'interfaccia di rete NVMf FC violata (ocumNvmfFcLifMbpsWarning)	Rischio	Interfaccia	Avvertimento

Eventi LUN

Gli eventi LUN forniscono informazioni sullo stato dei 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
LUN offline (ocumEvtLunOffline)	Incidente	LUN	Critico
LUN distrutto *(lunDestroy)	Evento	LUN	Informazioni
LUN mappato con sistema operativo non supportato in igroup(igroupUnsupportedOsType)	Incidente	LUN	Avvertimento
Singolo percorso attivo per accedere a LUN (ocumEvtLunSingleActivePath)	Rischio	LUN	Avvertimento
Nessun percorso attivo per accedere a LUN (ocumEvtLunNotReachable)	Incidente	LUN	Critico

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Nessun percorso ottimizzato per accedere a LUN (ocumEvtLunOptimizedPathInactive)	Rischio	LUN	Avvertimento
Nessun percorso per accedere a LUN dal partner HA (ocumEvtLunHaPathInactive)	Rischio	LUN	Avvertimento
Nessun percorso per accedere a LUN da un nodo in HA-pair (ocumEvtLunNodePathStatusDown)	Rischio	LUN	Errore

Area di impatto: capacità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Spazio insufficiente per la copia dello snapshot LUN (ocumEvtLunSnapshotNotPossible)	Rischio	Volume	Avvertimento

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
LUN mappato con sistema operativo non supportato in igroup(igroupUnsupportedOsType)	Rischio	LUN	Avvertimento

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica LUN IOPS violata (ocumLunIopsIncident)	Incidente	LUN	Critico

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia di avviso LUN IOPS superata (ocumLunIopsWarning)	Rischio	LUN	Avvertimento
Soglia critica LUN MB/s violata (ocumLunMbpsIncident)	Incidente	LUN	Critico
Soglia di avviso LUN MB/s superata (ocumLunMbpsWarning)	Rischio	LUN	Avvertimento
Soglia critica di latenza LUN ms/op violata (ocumLunLatencyIncident)	Incidente	LUN	Critico
Soglia di avviso di latenza LUN ms/op violata (ocumLunLatencyWarning)	Rischio	LUN	Avvertimento
Violazione della soglia critica di latenza LUN e IOPS (ocumLunLatencyIopsIncident)	Incidente	LUN	Critico
Soglia di avviso di latenza LUN e IOPS violata (ocumLunLatencyIopsWarning)	Rischio	LUN	Avvertimento
Latenza LUN e soglia critica MB/s violate (ocumLunLatencyMbpsIncident)	Incidente	LUN	Critico
Latenza LUN e soglia di avviso MB/s superate (ocumLunLatencyMbpsWarning)	Rischio	LUN	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica di latenza LUN e capacità di prestazioni aggregate utilizzata violata (ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incidente	LUN	Critico
Soglia di avviso per la latenza LUN e la capacità di prestazioni aggregate utilizzata superata (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Rischio	LUN	Avvertimento
Soglia critica di latenza LUN e utilizzo aggregato violata (ocumLunLatencyAggregateUtilizationIncident)	Incidente	LUN	Critico
Soglia di avviso di latenza LUN e utilizzo aggregato violata (ocumLunLatencyAggregateUtilizationWarning)	Rischio	LUN	Avvertimento
Soglia critica di latenza LUN e capacità di prestazioni del nodo utilizzata violata (ocumLunLatencyNodePerfCapacityUsedIncident)	Incidente	LUN	Critico
Soglia di avviso per la latenza LUN e la capacità delle prestazioni del nodo utilizzata superata (ocumLunLatencyNodePerfCapacityUsedWarning)	Rischio	LUN	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Latenza LUN e capacità di prestazioni del nodo utilizzata - Soglia critica di acquisizione violata (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	LUN	Critico
Latenza LUN e capacità di prestazioni del nodo utilizzata - Soglia di avviso di acquisizione violata (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Rischio	LUN	Avvertimento
Soglia critica di latenza LUN e utilizzo del nodo violata (ocumLunLatencyNodeUtilizationIncident)	Incidente	LUN	Critico
Soglia di avviso di latenza LUN e utilizzo del nodo violata (ocumLunLatencyNodeUtilizationWarning)	Rischio	LUN	Avvertimento
Soglia di avviso QoS LUN Max IOPS violata (ocumQosLunMaxIopsWarning)	Rischio	LUN	Avvertimento
Soglia di avviso QoS LUN Max MB/s violata (ocumQosLunMaxMbpsWarning)	Rischio	LUN	Avvertimento
Soglia di latenza LUN del carico di lavoro violata come definito dalla politica sul livello di servizio delle prestazioni (ocumConformanceLatencyWarning)	Rischio	LUN	Avvertimento

Eventi della stazione di gestione

Gli eventi della stazione 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Spazio su disco del server di gestione quasi pieno (ocumEvtUnifiedManager DiskSpaceNearlyFull)	Rischio	Stazione di gestione	Avvertimento
Spazio su disco del server di gestione pieno (ocumEvtUnifiedManager DiskSpaceFull)	Incidente	Stazione di gestione	Critico
Memoria insufficiente del server di gestione (ocumEvtUnifiedManager MemoryLow)	Rischio	Stazione di gestione	Avvertimento
Server di gestione quasi senza memoria (ocumEvtUnifiedManager MemoryAlmostOut)	Incidente	Stazione di gestione	Critico
Aumento delle dimensioni del file di registro MySQL; riavvio richiesto (ocumEvtMysqlLogFileSizeWarning)	Incidente	Stazione di gestione	Avvertimento
L'allocazione della dimensione totale del registro di controllo sta per essere completata	Rischio	Stazione di gestione	Avvertimento
Certificato del server Syslog in scadenza	Rischio	Stazione di gestione	Avvertimento
Certificato del server Syslog scaduto	Rischio	Stazione di gestione	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
File di registro di controllo manomesso	Rischio	Stazione di gestione	Avvertimento
File di registro di controllo eliminato	Rischio	Stazione di gestione	Avvertimento
Errore di connessione al server Syslog	Rischio	Stazione di gestione	Errore
Configurazione del server Syslog modificata	Evento	Stazione di gestione	Avvertimento

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
L'analisi dei dati sulle prestazioni è influenzata (ocumEvtUnifiedManager DataMissingAnalyze)	Rischio	Stazione di gestione	Avvertimento
La raccolta dei dati sulle prestazioni è influenzata (ocumEvtUnifiedManager DataMissingCollection)	Incidente	Stazione di gestione	Critico



Questi ultimi due eventi di performance erano disponibili solo per Unified Manager 7.2. Se uno di questi eventi è presente nello stato Nuovo e in seguito 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 Risolto.

Eventi MetroCluster Bridge

Gli eventi MetroCluster Bridge 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Ponte irraggiungibile (ocumEvtBridgeUnreachable)	Incidente	Ponte MetroCluster	Critico
Temperatura del ponte anomala (ocumEvtBridgeTemperatureAbnormal)	Incidente	Ponte 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 su FC e MetroCluster su IP, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Eventi comuni in entrambe le configurazioni

Questi eventi di connettività sono comuni sia alle configurazioni MetroCluster su FC che MetroCluster su IP.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Tutti i collegamenti tra i partner MetroCluster inattivi (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incidente	Relazione MetroCluster	Critico
Partner MetroCluster non raggiungibili tramite la rete di peering (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incidente	Relazione MetroCluster	Critico
Capacità di ripristino di emergenza MetroCluster compromessa (ocumEvtMetroClusterDRStatusImpacted)	Rischio	Relazione MetroCluster	Critico

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Configurazione MetroCluster commutata (ocumEvtMetroClusterDR StatusImpacted)	Rischio	Relazione MetroCluster	Avvertimento

Configurazione MetroCluster su FC

Questi eventi riguardano le configurazioni MetroCluster su FC.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Tutti i collegamenti tra switch inattivi (ocumEvtMetroClusterAll SLBetweenSwitchesDown)	Incidente	Collegamento inter-switch MetroCluster	Critico
Collegamento FC-SAS Bridge allo stack di archiviazione inattivo (ocumEvtBridgeSasPortDown)	Incidente	Collegamento dello stack del ponte MetroCluster	Critico
Configurazione MetroCluster parzialmente commutata (ocumEvtMetroClusterDR StatusPartiallyImpacted)	Rischio	Relazione MetroCluster	Errore
Da nodo a FC commuta tutti i collegamenti di interconnessione FC-VI inattivi (ocumEvtMccNodeSwitch FcviLinksDown)	Incidente	Connessione dello switch del nodo MetroCluster	Critico
Da nodo a FC commuta uno o più collegamenti FC-Initiator inattivi (ocumEvtMccNodeSwitch FcLinksOneOrMoreDown)	Rischio	Connessione dello switch del nodo MetroCluster	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Da nodo a FC, tutti i collegamenti FC-Initiator vengono interrotti (ocumEvtMccNodeSwitchFcLinksDown)	Incidente	Connessione dello switch del nodo MetroCluster	Critico
Passa al collegamento FC Bridge FC-SAS inattivo (ocumEvtMccSwitchBridgeFcLinksDown)	Incidente	Collegamento del ponte di commutazione MetroCluster	Critico
Inter Node Tutti i collegamenti FC VI InterConnect inattivi (ocumEvtMccInterNodeLinksDown)	Incidente	Connessione tra nodi	Critico
Inter Nodo Uno o più collegamenti di interconnessione FC VI inattivi (ocumEvtMccInterNodeLinksOneOrMoreDown)	Rischio	Connessione tra nodi	Avvertimento
Collegamento Nodo-Bridge inattivo (ocumEvtMccNodeBridgeLinksDown)	Incidente	Connessione del ponte del nodo	Critico
Nodo allo stack di archiviazione Tutti i collegamenti SAS inattivi (ocumEvtMccNodeStackLinksDown)	Incidente	Connessione dello stack dei nodi	Critico
Nodo allo stack di archiviazione Uno o più collegamenti SAS inattivi (ocumEvtMccNodeStackLinksOneOrMoreDown)	Rischio	Connessione dello stack dei nodi	Avvertimento

Configurazione MetroCluster su IP

Questi eventi riguardano le configurazioni MetroCluster su IP.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Lo stato di connettività intersito IP MetroCluster è inattivo (mccIntersiteconnectivityStatusDown)	Rischio	Relazione MetroCluster	Critico
MetroCluster- Nodo IP per commutare la connessione offline (mccIpPortStatusOffline)	Rischio	Nodo	Errore

Eventi di commutazione MetroCluster

Gli eventi dello switch MetroCluster per le configurazioni MetroCluster su FC forniscono informazioni sullo stato degli switch MetroCluster, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Temperatura di commutazione anomala (ocumEvtSwitchTemperatureAbnormal)	Incidente	Interruttore MetroCluster	Critico
Switch non raggiungibile (ocumEvtSwitchUnreachable)	Incidente	Interruttore MetroCluster	Critico
Ventole dello switch guaste (ocumEvtSwitchFansOneOrMoreFailed)	Incidente	Interruttore MetroCluster	Critico
Alimentatori Switch non funzionanti (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incidente	Interruttore MetroCluster	Critico

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Sensori di temperatura di commutazione non riusciti (ocumEvtSwitchTemperatureSensorFailed)  Questo evento è applicabile solo agli switch Cisco .	Incidente	Interruttore MetroCluster	Critico

Eventi dello spazio dei nomi NVMe

Gli eventi dello spazio dei nomi NVMe forniscono informazioni sullo stato dei tuoi 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
NVMeNS offline *(nvmeNamespaceStatusOffline)	Evento	Spazio dei nomi	Informazioni
NVMeNS Online *(nvmeNamespaceStatusOnline)	Evento	Spazio dei nomi	Informazioni
NVMeNS Spazio esaurito *(nvmeNamespaceSpaceOutOfSpace)	Rischio	Spazio dei nomi	Avvertimento
NVMeNS Destroy *(nvmeNamespaceDestroy)	Evento	Spazio dei nomi	Informazioni

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica IOPS dello spazio dei nomi NVMe violata (ocumNvmeNamespacelopsIncident)	Incidente	Spazio dei nomi	Critico
Soglia di avviso IOPS dello spazio dei nomi NVMe violata (ocumNvmeNamespacelopsWarning)	Rischio	Spazio dei nomi	Avvertimento
Soglia critica MB/s dello spazio dei nomi NVMe violata (ocumNvmeNamespaceMbpsIncident)	Incidente	Spazio dei nomi	Critico
Soglia di avviso MB/s dello spazio dei nomi NVMe violata (ocumNvmeNamespaceMbpsWarning)	Rischio	Spazio dei nomi	Avvertimento
Soglia critica di latenza dello spazio dei nomi NVMe ms/op violata (ocumNvmeNamespaceLatencyIncident)	Incidente	Spazio dei nomi	Critico
Soglia di avviso di latenza ms/op dello spazio dei nomi NVMe violata (ocumNvmeNamespaceLatencyWarning)	Rischio	Spazio dei nomi	Avvertimento
Soglia critica di latenza e IOPS dello spazio dei nomi NVMe violata (ocumNvmeNamespaceLatencyIopsIncident)	Incidente	Spazio dei nomi	Critico
Soglia di avviso di latenza e IOPS dello spazio dei nomi NVMe violata (ocumNvmeNamespaceLatencyIopsWarning)	Rischio	Spazio dei nomi	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Latenza dello spazio dei nomi NVMe e soglia critica MB/s violata (ocumNvmeNamespaceLatencyMbpsIncident)	Incidente	Spazio dei nomi	Critico
Soglia di avviso di latenza e MB/s dello spazio dei nomi NVMe violata (ocumNvmeNamespaceLatencyMbpsWarning)	Rischio	Spazio dei nomi	Avvertimento

Eventi del nodo

Gli eventi del nodo forniscono informazioni sullo stato del nodo, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Spazio del volume radice del nodo quasi pieno (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Rischio	Nodo	Avvertimento
Cloud AWS MetadataConnFail *(ocumCloudAwsMetadataConnFail)	Rischio	Nodo	Errore
Cloud AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Rischio	Nodo	Errore
Cloud AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Rischio	Nodo	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
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 Cloud Tier non risolvibile *(ocumObjstoreHostUnresolvable)	Rischio	Nodo	Errore
Interfaccia di rete intercluster Cloud Tier inattiva *(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 dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Memoria monitor QoS raggiunta al massimo *(ocumQosMonitorMemoryMaxed)	Rischio	Nodo	Errore
Memoria monitor QoS ridotta *(ocumQosMonitorMemoryAbated)	Evento	Nodo	Informazioni

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Nodo rinominato (non applicabile)	Evento	Nodo	Informazioni

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica IOPS del nodo violata (ocumNodeIopsIncident)	Incidente	Nodo	Critico
Soglia di avviso IOPS del nodo violata (ocumNodeIopsWarning)	Rischio	Nodo	Avvertimento
Soglia critica MB/s del nodo violata (ocumNodeMbpsIncident)	Incidente	Nodo	Critico
Soglia di avviso MB/s del nodo violata (ocumNodeMbpsWarning)	Rischio	Nodo	Avvertimento
Soglia critica di latenza del nodo ms/op violata (ocumNodeLatencyIncident)	Incidente	Nodo	Critico

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia di avviso di latenza del nodo ms/op violata (ocumNodeLatencyWarning)	Rischio	Nodo	Avvertimento
Capacità di prestazioni del nodo utilizzata soglia critica violata (ocumNodePerfCapacityUsedIncident)	Incidente	Nodo	Critico
Soglia di avviso relativa alla capacità di prestazioni del nodo utilizzata superata (ocumNodePerfCapacityUsedWarning)	Rischio	Nodo	Avvertimento
Capacità di prestazioni del nodo utilizzata - Soglia critica di acquisizione violata (ocumNodePerfCapacityUsedTakeoverIncident)	Incidente	Nodo	Critico
Capacità di prestazioni del nodo utilizzata - Soglia di avviso di acquisizione violata (ocumNodePerfCapacityUsedTakeoverWarning)	Rischio	Nodo	Avvertimento
Soglia critica di utilizzo del nodo violata (ocumNodeUtilizationIncident)	Incidente	Nodo	Critico
Soglia di avviso di utilizzo del nodo superata (ocumNodeUtilizationWarning)	Rischio	Nodo	Avvertimento
Soglia di sovrautilizzo della coppia di nodi HA violata (ocumNodeHaPairOverUtilizedInformation)	Evento	Nodo	Informazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia di frammentazione del disco del nodo violata (ocumNodeDiskFragmentationWarning)	Rischio	Nodo	Avvertimento
Superata la soglia di capacità di prestazione utilizzata (ocumNodeOverUtilizedWarning)	Rischio	Nodo	Avvertimento
Soglia dinamica del nodo violata (ocumNodeDynamicEventWarning)	Rischio	Nodo	Avvertimento

Area di impatto: sicurezza

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
ID avviso: NTAP- <i><ID avviso></i> (ocumx)	Rischio	Nodo	Critico

Eventi della batteria NVRAM

Gli eventi della batteria NVRAM forniscono informazioni sullo stato delle batterie, consentendo di monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Batteria NVRAM scarica (ocumEvtNvramBatteryLow)	Rischio	Nodo	Avvertimento
Batteria NVRAM scarica (ocumEvtNvramBatteryDischarged)	Rischio	Nodo	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Batteria NVRAM eccessivamente carica (ocumEvtNvramBatteryOverCharged)	Incidente	Nodo	Critico

Eventi portuali

Gli eventi delle porte forniscono informazioni sullo stato delle porte del cluster, in modo da poter monitorare modifiche o problemi sulla porta, ad esempio se la porta è inattiva.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Stato della porta inattivo (ocumEvtPortStatusDown)	Incidente	Nodo	Critico

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica MB/s della porta di rete violata (ocumNetworkPortMbpsIncident)	Incidente	Porta	Critico
Soglia di avviso MB/s della porta di rete violata (ocumNetworkPortMbpsWarning)	Rischio	Porta	Avvertimento
Soglia critica MB/s della porta FCP violata (ocumFcpPortMbpsIncident)	Incidente	Porta	Critico
Soglia di avviso MB/s della porta FCP violata (ocumFcpPortMbpsWarning)	Rischio	Porta	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica di utilizzo della porta di rete violata (ocumNetworkPortUtilizationIncident)	Incidente	Porta	Critico
Soglia di avviso per l'utilizzo della porta di rete violata (ocumNetworkPortUtilizationWarning)	Rischio	Porta	Avvertimento
Soglia critica di utilizzo della porta FCP violata (ocumFcpPortUtilizationIncident)	Incidente	Porta	Critico
Soglia di avviso di utilizzo della porta FCP violata (ocumFcpPortUtilizationWarning)	Rischio	Porta	Avvertimento

Eventi di alimentazione

Gli eventi degli alimentatori forniscono informazioni sullo stato dell'hardware, consentendo di monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Uno o più alimentatori guasti (ocumEvtPowerSupplyOneOrMoreFailed)	Incidente	Nodo	Critico

Eventi di protezione

Gli eventi di protezione ti informano se un processo non è riuscito o è stato interrotto, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: protezione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Processo di protezione non riuscito (ocumEvtProtectionJobTaskFailed)	Incidente	Servizio di volume o di stoccaggio	Critico
Lavoro di protezione interrotto (ocumEvtProtectionJobAborted)	Rischio	Servizio di volume o di stoccaggio	Avvertimento

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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: capacità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Spazio Qtree quasi pieno (ocumEvtQtreeSpaceNearlyFull)	Rischio	Qtree	Avvertimento
Spazio Qtree pieno (ocumEvtQtreeSpaceFull)	Rischio	Qtree	Errore
Qtree Space Normal(ocumEvtQtreeSpaceThresholdOk)	Evento	Qtree	Informazioni
Limite massimo dei file Qtree raggiunto (ocumEvtQtreeFilesHardLimitReached)	Incidente	Qtree	Critico
Limite flessibile dei file Qtree violato (ocumEvtQtreeFilesSoftLimitBreached)	Rischio	Qtree	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Limite massimo di spazio Qtree raggiunto (ocumEvtQtreeSpaceHardLimitReached)	Incidente	Qtree	Critico
Limite flessibile dello spazio Qtree violato (ocumEvtQtreeSpaceSoftLimitBreached)	Rischio	Qtree	Avvertimento

Eventi del processore di servizio

Gli eventi del processore di servizio 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Processore di servizio non configurato (ocumEvtServiceProcessorNotConfigured)	Rischio	Nodo	Avvertimento
Processore di servizio offline (ocumEvtServiceProcessorOffline)	Rischio	Nodo	Errore

Eventi di relazione SnapMirror

Gli eventi di relazione SnapMirror forniscono informazioni sullo stato delle relazioni SnapMirror asincrone e sincrone, in modo da poter monitorare eventuali problemi. Gli eventi di relazione SnapMirror asincroni vengono generati sia per le VM di archiviazione che per i volumi, mentre 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 ripristino di emergenza della VM di archiviazione. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trappola, il livello di impatto, il tipo di origine e la gravità.

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 archiviazione protette dal ripristino di emergenza delle VM di archiviazione, ma non per le relazioni tra oggetti costituenti.

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Replica dello specchio non funzionante (ocumEvtSnapmirrorRelationshipUnhealthy)	Rischio	Relazione SnapMirror	Avvertimento
Replicazione speculare interrotta (ocumEvtSnapmirrorRelationshipStateBrokenoff)	Rischio	Relazione SnapMirror	Errore
Inizializzazione della replica mirror non riuscita (ocumEvtSnapmirrorRelationshipInitializeFailed)	Rischio	Relazione SnapMirror	Errore
Aggiornamento della replica mirror non riuscito (ocumEvtSnapmirrorRelationshipUpdateFailed)	Rischio	Relazione SnapMirror	Errore
Errore di ritardo della replica mirror (ocumEvtSnapMirrorRelationshipLagError)	Rischio	Relazione SnapMirror	Errore
Avviso di ritardo nella replica dello specchio (ocumEvtSnapMirrorRelationshipLagWarning)	Rischio	Relazione SnapMirror	Avvertimento
Risincronizzazione della replica mirror non riuscita (ocumEvtSnapmirrorRelationshipResyncFailed)	Rischio	Relazione SnapMirror	Errore
Replica sincrona fuori sincrono *(syncSnapmirrorRelationshipOutofsync)	Rischio	Relazione SnapMirror	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Replica sincrona ripristinata *(syncSnapmirrorRelationshipInSync)	Evento	Relazione SnapMirror	Informazioni
Replica sincrona: risincronizzazione automatica non riuscita *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Rischio	Relazione SnapMirror	Errore
Ontap Mediator è stato aggiunto al cluster (snapmirrorMediatorAdded)	Evento	Grappolo	Informazioni
Ontap Mediator è stato rimosso dal cluster (snapmirrorMediatorRemoved)	Evento	Grappolo	Informazioni
Ontap Mediator non è raggiungibile dal cluster (snapmirrorMediatorUnreachable)	Rischio	Mediatore	Avvertimento
Ontap Mediator non è accessibile dal cluster (snapmirrorMediatorMisconfigured)	Rischio	Mediatore	Errore
La connettività di Ontap Mediator è stata ristabilita, è risincronizzata ed è pronta per la sincronizzazione attiva SnapMirror (snapmirrorMediatorInQuorum)	Evento	Mediatore	Informazioni

Eventi di relazione asincroni Mirror e Vault

Gli eventi di relazione Asynchronous Mirror e Vault forniscono informazioni sullo stato delle relazioni Asynchronous SnapMirror e Vault, in modo da poter monitorare potenziali problemi. Gli eventi di relazione Mirror e Vault asincroni sono supportati sia per le relazioni di protezione dei volumi che per quelle delle VM di archiviazione. Tuttavia, solo le relazioni Vault non sono supportate per il ripristino di emergenza delle VM di

archiviazione. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: protezione



Gli eventi di relazione SnapMirror e Vault vengono generati anche per le VM di archiviazione protette dal ripristino di emergenza delle VM di archiviazione, ma non per le relazioni tra oggetti costituenti.

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Mirror asincrono e Vault non integri (ocumEvtMirrorVaultRelationshipUnhealthy)	Rischio	Relazione SnapMirror	Avvertimento
Mirror asincrono e Vault interrotti (ocumEvtMirrorVaultRelationshipStateBrokenoff)	Rischio	Relazione SnapMirror	Errore
Inizializzazione mirror e vault asincroni non riuscita (ocumEvtMirrorVaultRelationshipInitializeFailed)	Rischio	Relazione SnapMirror	Errore
Aggiornamento asincrono di mirror e vault non riuscito (ocumEvtMirrorVaultRelationshipUpdateFailed)	Rischio	Relazione SnapMirror	Errore
Errore di ritardo di mirroring e vault asincroni (ocumEvtMirrorVaultRelationshipLagError)	Rischio	Relazione SnapMirror	Errore
Avviso di ritardo di mirroring e vault asincroni (ocumEvtMirrorVaultRelationshipLagWarning)	Rischio	Relazione SnapMirror	Avvertimento
Mirror asincrono e risincronizzazione del vault non riusciti (ocumEvtMirrorVaultRelationshipResyncFailed)	Rischio	Relazione SnapMirror	Errore



L'evento "Errore di aggiornamento SnapMirror " viene generato dal portale Active IQ (Config Advisor).

Eventi snapshot

Gli eventi snapshot forniscono informazioni sullo stato degli snapshot, consentendo di monitorarli per individuare potenziali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento, il nome della trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Eliminazione automatica snapshot disabilitata (non applicabile)	Evento	Volume	Informazioni
Eliminazione automatica snapshot abilitata (non applicabile)	Evento	Volume	Informazioni
Configurazione di eliminazione automatica 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: protezione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Vault asincrono non integro (ocumEvtSnapVaultRelationshipUnhealthy)	Rischio	Relazione SnapMirror	Avvertimento
Vault asincrono interrotto (ocumEvtSnapVaultRelationshipStateBrokenoff)	Rischio	Relazione SnapMirror	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Inizializzazione del vault asincrono non riuscita (ocumEvtSnapVaultRelationshipInitializeFailed)	Rischio	Relazione SnapMirror	Errore
Aggiornamento asincrono del vault non riuscito (ocumEvtSnapVaultRelationshipUpdateFailed)	Rischio	Relazione SnapMirror	Errore
Errore di ritardo del vault asincrono (ocumEvtSnapVaultRelationshipLagError)	Rischio	Relazione SnapMirror	Errore
Avviso di ritardo del vault asincrono (ocumEvtSnapVaultRelationshipLagWarning)	Rischio	Relazione SnapMirror	Avvertimento
Risincronizzazione asincrona del vault non riuscita (ocumEvtSnapvaultRelationshipResyncFailed)	Rischio	Relazione SnapMirror	Errore

Eventi delle impostazioni di failover dell'archiviazione

Gli eventi delle impostazioni di failover dell'archiviazione (SFO) forniscono informazioni sulla disattivazione o meno del failover dell'archiviazione, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Interconnessione failover di archiviazione Uno o più collegamenti inattivi (ocumEvtSfoInterconnectOneOrMoreLinksDown)	Rischio	Nodo	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Failover di archiviazione disabilitato (ocumEvtSfoSettingsDisabled)	Rischio	Nodo	Errore
Failover di archiviazione non configurato (ocumEvtSfoSettingsNotConfigured)	Rischio	Nodo	Errore
Stato di failover dell'archiviazione - Takeover(ocumEvtSfoStateTakeover)	Rischio	Nodo	Avvertimento
Stato di failover dell'archiviazione - Restituzione parziale (ocumEvtSfoStatePartialGiveback)	Rischio	Nodo	Errore
Stato del nodo di failover di archiviazione inattivo (ocumEvtSfoNodeStatusDown)	Rischio	Nodo	Errore
Acquisizione del failover di archiviazione non possibile (ocumEvtSfoTakeoverNotPossible)	Rischio	Nodo	Errore

Eventi sui servizi di stoccaggio

Gli eventi dei servizi di archiviazione forniscono informazioni sulla creazione e la sottoscrizione di servizi di archiviazione, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Servizio di archiviazione creato (non applicabile)	Evento	Servizio di deposito	Informazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Servizio di archiviazione sottoscritto (non applicabile)	Evento	Servizio di deposito	Informazioni
Servizio di archiviazione annullato (non applicabile)	Evento	Servizio di deposito	Informazioni

Area di impatto: protezione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Eliminazione imprevista di Managed SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	Rischio	Servizio di deposito	Avvertimento
Eliminazione imprevista del volume membro del servizio di archiviazione (ocumEvtStorageService UnexpectedVolumeDeletion)	Incidente	Servizio di deposito	Critico

Eventi sugli scaffali di stoccaggio

Gli eventi sullo scaffale di stoccaggio ti informano se lo scaffale presenta anomalie, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Intervallo di tensione anomalo (ocumEvtShelfVoltageAbnormal)	Rischio	Scaffale portaoggetti	Avvertimento
Intervallo di corrente anormale (ocumEvtShelfCurrentAbnormal)	Rischio	Scaffale portaoggetti	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Temperatura anomala (ocumEvtShelfTemperatureAbnormal)	Rischio	Scaffale portaoggetti	Avvertimento

Eventi VM di archiviazione

Gli eventi Storage VM (macchina virtuale di archiviazione, nota anche come SVM) forniscono informazioni sullo stato delle VM di archiviazione (SVM), 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Servizio CIFS VM di archiviazione inattivo (ocumEvtVserverCifsServiceStatusDown)	Incidente	SVM	Critico
Servizio CIFS SVM non configurato (non applicabile)	Evento	SVM	Informazioni
Tentativi di connessione a condivisione CIFS inesistente *(nbladeCifsNoPrivShare)	Incidente	SVM	Critico
Conflitto di nomi NetBIOS CIFS *(nbladeCifsNbNameConflict)	Rischio	SVM	Errore
Operazione di copia shadow CIFS non riuscita *(cifsShadowCopyFailure)	Rischio	SVM	Errore
Molte connessioni CIFS *(nbladeCifsManyAuths)	Rischio	SVM	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Numero massimo di connessioni CIFS superato *(nbladeCifsMaxOpenSameFile)	Rischio	SVM	Errore
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
Servizio NFS VM di archiviazione inattivo (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
VM di archiviazione arrestata (ocumEvtVserverDown)	Rischio	SVM	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Il server AV è troppo occupato per accettare una nuova richiesta di scansione *(nbladeVscanConnBackPressure)	Rischio	SVM	Errore
Nessuna connessione al server AV per la scansione antivirus *(nbladeVscanNoScannerConn)	Incidente	SVM	Critico
Nessun server AV registrato *(nbladeVscanNoRegdScanner)	Rischio	SVM	Errore
Nessuna connessione al server AV reattivo *(nbladeVscanConnInactive)	Evento	SVM	Informazioni
Tentativo di accesso non autorizzato al server AV *(nbladeVscanBadUserPrivAccess)	Rischio	SVM	Errore
Virus trovato dal server AV *(nbladeVscanVirusDetected)	Rischio	SVM	Errore

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
SVM scoperto (non applicabile)	Evento	SVM	Informazioni
SVM eliminato (non applicabile)	Evento	Grappolo	Informazioni
SVM rinominato (non applicabile)	Evento	SVM	Informazioni

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica SVM IOPS violata (ocumSvmIopsIncident)	Incidente	SVM	Critico
Soglia di avviso IOPS SVM violata (ocumSvmIopsWarning)	Rischio	SVM	Avvertimento
Soglia critica SVM MB/s violata (ocumSvmMbpsIncident)	Incidente	SVM	Critico
Soglia di avviso MB/s SVM violata (ocumSvmMbpsWarning)	Rischio	SVM	Avvertimento
Soglia critica di latenza SVM violata (ocumSvmLatencyIncident)	Incidente	SVM	Critico
Soglia di avviso di latenza SVM violata (ocumSvmLatencyWarning)	Rischio	SVM	Avvertimento

Area di impatto: sicurezza

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Registro di controllo disabilitato (ocumVserverAuditLogDisabled)	Rischio	SVM	Avvertimento
Banner di accesso disabilitato (ocumVserverLoginBannerDisabled)	Rischio	SVM	Avvertimento
SSH utilizza cifrari non sicuri (ocumVserverSSHInsecure)	Rischio	SVM	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Banner di accesso modificato (ocumVserverLoginBannerChanged)	Rischio	SVM	Avvertimento
Il monitoraggio anti-ransomware della VM di archiviazione è disabilitato (antiRansomwareSvmStateDisabled)	Rischio	SVM	Avvertimento
Il monitoraggio anti-ransomware della VM di archiviazione è abilitato (modalità di apprendimento) (antiRansomwareSvmStateDryrun)	Evento	SVM	Informazioni
VM di archiviazione adatta al monitoraggio anti-ransomware (modalità di apprendimento) (ocumEvtSvmArwCandidate)	Evento	SVM	Informazioni

Eventi di quota utente e gruppo

Gli eventi relativi alle quote utente e gruppo forniscono informazioni sulla capacità della quota utente e gruppo utente, nonché sui limiti di file e disco, 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: capacità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Limite flessibile dello spazio su disco della quota utente o gruppo violato (ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Rischio	Quota utente o gruppo	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Limite massimo di spazio su disco per utente o gruppo raggiunto (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incidente	Quota utente o gruppo	Critico
Limite flessibile del numero di file della quota utente o gruppo violato (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Rischio	Quota utente o gruppo	Avvertimento
Limite massimo di conteggio file quota utente o gruppo raggiunto (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incidente	Quota utente o gruppo	Critico

Eventi di volume

Gli eventi del volume forniscono informazioni sullo stato dei volumi, consentendo di monitorare potenziali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento, il nome della trappola, il livello di impatto, il tipo di origine e la gravità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: disponibilità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Volume limitato (ocumEvtVolumeRestricted)	Rischio	Volume	Avvertimento
Volume offline (ocumEvtVolumeOffline)	Incidente	Volume	Critico
Volume parzialmente disponibile (ocumEvtVolumePartiallyAvailable)	Rischio	Volume	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Volume non montato (non applicabile)	Evento	Volume	Informazioni
Volume montato (non applicabile)	Evento	Volume	Informazioni
Volume rimontato (non applicabile)	Evento	Volume	Informazioni
Percorso di giunzione del volume inattivo (ocumEvtVolumeJunctionPathInactive)	Rischio	Volume	Avvertimento
Ridimensionamento automatico del volume abilitato (non applicabile)	Evento	Volume	Informazioni
Volume Autosize-Disabilitato (non applicabile)	Evento	Volume	Informazioni
Volume Autosize Capacità massima modificata (non applicabile)	Evento	Volume	Informazioni
Incremento automatico del volume Dimensione modificata (non applicabile)	Evento	Volume	Informazioni

Area di impatto: capacità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Spazio del volume con provisioning sottile a rischio (ocumThinProvisionVolumeSpaceAtRisk)	Rischio	Volume	Avvertimento
Errore di funzionamento dell'efficienza del volume (ocumEvtVolumeEfficiencyOperationError)	Rischio	Volume	Errore

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Spazio volume pieno (ocumEvtVolumeFull)	Rischio	Volume	Errore
Spazio volume quasi pieno (ocumEvtVolumeNearlyFull)	Rischio	Volume	Avvertimento
Spazio logico del volume pieno (volumeLogicalSpaceFull)	Rischio	Volume	Errore
Spazio logico del volume quasi pieno (volumeLogicalSpaceNearlyFull)	Rischio	Volume	Avvertimento
Volume Spazio logico normale (volumeLogicalSpaceAllOK)	Evento	Volume	Informazioni
Spazio di riserva dello snapshot del volume pieno (ocumEvtSnapshotFull)	Rischio	Volume	Avvertimento
Troppe copie di snapshot (ocumEvtSnapshotTooMany)	Rischio	Volume	Errore
Quota Qtree del volume superata (ocumEvtVolumeQtreeQuotaOvercommitted)	Rischio	Volume	Errore
Quota Qtree del volume quasi superata (ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Rischio	Volume	Avvertimento
Tasso di crescita del volume anomalo (ocumEvtVolumeGrowthRateAbnormal)	Rischio	Volume	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Volume Giorni Fino al Pieno (ocumEvtVolumeDaysUntilFullSoon)	Rischio	Volume	Errore
Garanzia di spazio volume disabilitata (non applicabile)	Evento	Volume	Informazioni
Garanzia di spazio volume abilitata (non applicabile)	Evento	Volume	Informazioni
Garanzia di spazio volume modificata (non applicabile)	Evento	Volume	Informazioni
Giorni di riserva dello snapshot del volume fino al riempimento (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Rischio	Volume	Errore
I componenti di FlexGroup hanno problemi di spazio (flexGroupConstituentsHaveSpaceIssues)	Rischio	Volume	Errore
Stato dello spazio dei componenti FlexGroup Tutto OK (flexGroupConstituentsSpaceStatusAllOK)	Evento	Volume	Informazioni
I costituenti FlexGroup hanno problemi con gli inode (flexGroupConstituentsHaveNodesIssues)	Rischio	Volume	Errore
FlexGroup Costituenti Inodes Stato Tutto OK (flexGroupConstituentsInodesStatusAllOK)	Evento	Volume	Informazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Errore di ridimensionamento automatico del volume WAFL *(wafIVolAutoSizeFail)	Rischio	Volume	Errore
WAFL Volume AutoSize Done *(wafIVolAutoSizeDone)	Evento	Volume	Informazioni
Il volume FlexGroup è utilizzato per oltre l'80%*	Incidente	Volume	Errore
Il volume FlexGroup è utilizzato per oltre il 90%*	Incidente	Volume	Critico
Anomalia nell'efficienza di archiviazione del volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Rischio	Volume	Avvertimento
Riserva snapshot del volume sottoutilizzata (volumeSnaphotReserveUnderutilizedWarning)	Evento	Volume	Avvertimento
Riserva snapshot del volume sottoutilizzata (volumeSnaphotReserveUnderutilizedCleared)	Evento	Volume	Avvertimento

Area di impatto: configurazione

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Volume rinominato (non applicabile)	Evento	Volume	Informazioni
Volume scoperto (non applicabile)	Evento	Volume	Informazioni
Volume eliminato (non applicabile)	Evento	Volume	Informazioni

Area di impatto: prestazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia di avviso IOPS massimi del volume QoS violata (ocumQosVolumeMaxlopsWarning)	Rischio	Volume	Avvertimento
Soglia di avviso massima MB/s del volume QoS violata (ocumQosVolumeMaxMbpsWarning)	Rischio	Volume	Avvertimento
Soglia di avviso massima IOPS/TB del volume QoS violata (ocumQosVolumeMaxlopsPerTbWarning)	Rischio	Volume	Avvertimento
Soglia di latenza del volume del carico di lavoro violata come definito dalla politica sul livello di servizio delle prestazioni (ocumConformanceLatencyWarning)	Rischio	Volume	Avvertimento
Soglia critica di IOPS del volume violata (ocumVolumelopsIncident)	Incidente	Volume	Critico
Soglia di avviso IOPS del volume superata (ocumVolumelopsWarning)	Rischio	Volume	Avvertimento
Soglia critica del volume MB/s violata (ocumVolumeMbpsIncident)	Incidente	Volume	Critico
Soglia di avviso volume MB/s superata (ocumVolumeMbpsWarning)	Rischio	Volume	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica di latenza del volume violata (ocumVolumeLatencyIncident)	Incidente	Volume	Critico
Soglia di avviso di latenza del volume superata (ocumVolumeLatencyWarning)	Rischio	Volume	Avvertimento
Soglia critica del rapporto di mancata esecuzione della cache del volume violata (ocumVolumeCacheMissRatioIncident)	Incidente	Volume	Critico
Soglia di avviso per il rapporto di mancata esecuzione della cache del volume violata (ocumVolumeCacheMissRatioWarning)	Rischio	Volume	Avvertimento
Soglia critica di latenza del volume e IOPS violata (ocumVolumeLatencyIopsIncident)	Incidente	Volume	Critico
Soglia di avviso di latenza del volume e IOPS violata (ocumVolumeLatencyIopsWarning)	Rischio	Volume	Avvertimento
Latenza del volume e soglia critica MB/s violate (ocumVolumeLatencyMbpsIncident)	Incidente	Volume	Critico
Latenza del volume e soglia di avviso MB/s superata (ocumVolumeLatencyMbpsWarning)	Rischio	Volume	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Soglia critica di latenza del volume e capacità di prestazioni aggregate utilizzata violata (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incidente	Volume	Critico
Soglia di avviso per la latenza del volume e la capacità di prestazioni aggregate utilizzata superata (ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Rischio	Volume	Avvertimento
Soglia critica di latenza del volume e utilizzo aggregato violata (ocumVolumeLatencyAggregateUtilizationIncident)	Incidente	Volume	Critico
Soglia di avviso per latenza del volume e utilizzo aggregato violata (ocumVolumeLatencyAggregateUtilizationWarning)	Rischio	Volume	Avvertimento
Soglia critica di latenza del volume e capacità di prestazioni del nodo utilizzata violata (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incidente	Volume	Critico
Soglia di avviso per la latenza del volume e la capacità delle prestazioni del nodo utilizzata superata (ocumVolumeLatencyNodePerfCapacityUsedWarning)	Rischio	Volume	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Latenza del volume e capacità di prestazioni del nodo utilizzata - Soglia critica di acquisizione violata (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	Volume	Critico
Latenza del volume e capacità di prestazioni del nodo utilizzata - Soglia di avviso di acquisizione violata (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Rischio	Volume	Avvertimento
Soglia critica di latenza del volume e utilizzo del nodo violata (ocumVolumeLatencyNodeUtilizationIncident)	Incidente	Volume	Critico
Soglia di avviso per latenza del volume e utilizzo del nodo superata (ocumVolumeLatencyNodeUtilizationWarning)	Rischio	Volume	Avvertimento

Area di impatto: sicurezza

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Il monitoraggio anti-ransomware del volume è abilitato (modalità attiva) (antiRansomwareVolumeStateEnabled)	Evento	Volume	Informazioni
Il monitoraggio anti-ransomware del volume è disabilitato (antiRansomwareVolumeStateDisabled)	Rischio	Volume	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Il monitoraggio anti-ransomware del volume è abilitato (modalità di apprendimento) (antiRansomwareVolumeStateDryrun)	Evento	Volume	Informazioni
Il monitoraggio anti-ransomware del volume è in pausa (modalità di apprendimento) (antiRansomwareVolumeStateDryrunPaused)	Rischio	Volume	Avvertimento
Il monitoraggio anti-ransomware del volume è in pausa (modalità attiva) (antiRansomwareVolumeStateEnablePaused)	Rischio	Volume	Avvertimento
Il monitoraggio anti-ransomware del volume è disabilitato (antiRansomwareVolumeStateDisableInProgress)	Rischio	Volume	Avvertimento
Attività ransomware rilevata (callHomeRansomwareActivitySeen)	Incidente	Volume	Critico
Volume adatto al monitoraggio anti-ransomware (modalità di apprendimento) (ocumEvtVolumeArwCandidates)	Evento	Volume	Informazioni
Volume adatto al monitoraggio anti-ransomware (modalità attiva) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Rischio	Volume	Avvertimento

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Il volume mostra avvisi anti-ransomware rumorosi (antiRansomwareFeature NoisyVolume)	Rischio	Volume	Avvertimento

Area di impatto: protezione dei dati

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Il volume non ha una protezione snapshot locale sufficiente (volumeLacksLocalProtectionWarning)	Rischio	Volume	Avvertimento
Il volume non ha una protezione snapshot locale sufficiente (volumeLacksLocalProtectionCleared)	Rischio	Volume	Avvertimento

Eventi di stato di spostamento del volume

Gli eventi sullo stato dello spostamento del volume ti informano sullo 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 trappola, il livello di impatto, il tipo di origine e la gravità.

Area di impatto: capacità

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Stato dello spostamento del volume: in corso (non applicabile)	Evento	Volume	Informazioni
Stato spostamento volume - Fallito (ocumEvtVolumeMoveFailed)	Rischio	Volume	Errore
Stato del trasferimento del volume: completato (non applicabile)	Evento	Volume	Informazioni

Nome dell'evento (nome della trappola)	Livello di impatto	Tipo di fonte	Gravità
Spostamento del volume - Cutover differito (ocumEvtVolumeMoveCutoverDeferred)	Rischio	Volume	Avvertimento

Descrizione delle finestre degli eventi e delle finestre di dialogo

Gli eventi ti informano su eventuali problemi nel tuo ambiente. È possibile utilizzare la pagina dell'inventario Gestione eventi e la pagina Dettagli evento per monitorare tutti gli eventi. È possibile utilizzare la finestra di dialogo Opzioni di configurazione delle notifiche per configurare le notifiche. È possibile utilizzare la pagina Impostazione evento per disabilitare o abilitare 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 anche possibile configurare i meccanismi di notifica. Ad esempio, le notifiche possono essere inviate tramite e-mail o trap SNMP.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

E-mail

Quest'area consente di configurare le seguenti impostazioni e-mail per la notifica degli avvisi:

- **Da Indirizzo**

Specifica l'indirizzo email da cui viene inviata la notifica di avviso. Questo valore viene utilizzato anche come indirizzo del mittente per un report quando viene condiviso. Se l'indirizzo del mittente è precompilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", dovresti modificarlo con un indirizzo email reale e funzionante per assicurarti che tutte le notifiche email vengano recapitate correttamente.

Server SMTP

Quest'area 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 quando SMTPAUTH è abilitato nel server SMTP.

- **Password**

Specifica la password SMTP. Il nome utente SMTP è obbligatorio solo quando SMTPAUTH è abilitato nel server SMTP.

- **Porta**

Specifica la porta utilizzata dal server host SMTP per inviare notifiche di avviso.

Il valore predefinito è 25.

- **Usa START/TLS**

Selezionando questa casella si garantisce una comunicazione sicura tra il server SMTP e il server di gestione mediante l'utilizzo dei protocolli TLS/SSL (noti anche come start_tls e StartTLS).

- **Usa SSL**

Selezionando questa casella si garantisce una comunicazione sicura tra il server SMTP e il server di gestione mediante l'utilizzo del protocollo SSL.

SNMP

Quest'area consente di configurare le seguenti impostazioni trap SNMP:

- **Versione**

Specifica la versione SNMP che si desidera utilizzare a seconda del tipo di sicurezza richiesto. Le opzioni includono la versione 1, la versione 3, la versione 3 con autenticazione e la versione 3 con autenticazione e crittografia. Il valore predefinito è Versione 1.

- **Host di destinazione della trappola**

Specifica il nome host o l'indirizzo IP (IPv4 o IPv6) che riceve le trap SNMP inviate dal server di gestione. Per specificare più destinazioni trap, separare ogni host con una virgola.



Tutte le altre impostazioni SNMP, come "Versione" e "Porta in uscita", devono essere le stesse per tutti gli host nell'elenco.

- **Porta trappola in uscita**

Specifica la porta attraverso la quale il server SNMP riceve le trap inviate dal server di gestione.

Il valore predefinito è 162.

- **Comunità**

Stringa della community 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 di 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 di protocollo includono AES 128 e DES. Il valore predefinito è AES 128. Il protocollo di privacy è disponibile con SNMP versione 3 con autenticazione e crittografia.

- **Password di riservatezza**

Specifica la password quando si utilizza il protocollo di privacy. La password di privacy è disponibile con SNMP versione 3 con autenticazione e crittografia.

Per ulteriori informazioni sugli oggetti e le trappole SNMP, è possibile scaricare il "[MIB Active IQ Unified Manager](#)" dal sito di supporto NetApp .

Pagina dell'inventario di gestione degli eventi

La pagina dell'inventario Gestione eventi consente di visualizzare un elenco degli eventi correnti e delle relative proprietà. È possibile eseguire attività quali il riconoscimento, la risoluzione e l'assegnazione di eventi. Puoi anche aggiungere un avviso per eventi specifici.

Le informazioni presenti in questa pagina vengono aggiornate automaticamente ogni 5 minuti per garantire che vengano visualizzati gli 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:

- Visualizza il menu per selezionare da un elenco predefinito di selezioni di filtri.

Ciò include elementi quali tutti gli eventi attivi (nuovi e riconosciuti), gli eventi di prestazioni attivi, gli eventi assegnati a me (l'utente registrato) e tutti gli eventi generati durante tutte le finestre di manutenzione.

- Riquadro di ricerca per restringere l'elenco degli eventi inserendo termini completi o parziali.
- Pulsante Filtro che avvia il riquadro Filtri, in modo da poter selezionare tutti i campi e gli attributi di campo disponibili per perfezionare l'elenco degli eventi.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Assegna a**

Consente di selezionare l'utente a cui assegnare l'evento. Quando assegni un evento a un utente, il nome utente e l'ora in cui hai assegnato l'evento vengono aggiunti all'elenco degli eventi selezionati.

- Me

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 anche possibile annullare l'assegnazione degli eventi lasciando vuoto il campo della proprietà.

- **Riconoscere**

Riconosce gli eventi selezionati.

Quando si riconosce un evento, il nome utente e l'ora in cui è stato riconosciuto l'evento vengono aggiunti all'elenco degli eventi selezionati. Quando riconosci un evento, sei responsabile della gestione di quell'evento.



Non è possibile riconoscere gli eventi informativi.

- **Segna come risolto**

Consente di modificare lo stato dell'evento in risolto.

Quando risolvi un evento, il tuo nome utente e l'ora in cui hai risolto l'evento vengono aggiunti all'elenco degli eventi selezionati. Dopo aver adottato misure correttive 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.

- **Segnalazioni**

Consente di esportare i dettagli della vista dell'evento corrente in un file con valori separati da virgole (.csv) o in un documento PDF.

- **Mostra/Nascondi selettore di colonna**

Consente di scegliere le colonne da visualizzare sulla pagina e di selezionare l'ordine in cui visualizzarle.

Elenco degli eventi

Visualizza i dettagli di tutti gli eventi ordinati in base all'ora di attivazione.

Per impostazione predefinita, viene visualizzata la vista Tutti gli eventi attivi per mostrare gli eventi Nuovi e Riconosciuti dei sette giorni precedenti che hanno un Livello di impatto di Incidente o Rischio.

- **Tempo di attivazione**

Ora in cui è stato generato l'evento.

- **Gravità**

Gravità dell'evento: Critico (❌), Errore (⚠️), Avvertimento (⚠️), e Informazioni (ℹ️).

- **Stato**

Stato dell'evento: Nuovo, Riconosciuto, Risolto o Obsoleto.

- **Livello di impatto**

Livello di impatto dell'evento: incidente, rischio, evento o aggiornamento.

- **Area di impatto**

Area di impatto dell'evento: disponibilità, capacità, prestazioni, protezione, configurazione o sicurezza.

- **Nome**

Il nome dell'evento. È possibile selezionare il nome per visualizzare la pagina dei dettagli dell'evento.

- **Fonte**

Il nome dell'oggetto su cui si è verificato l'evento. È possibile selezionare il nome per visualizzare la pagina dei dettagli sullo stato o sulle prestazioni di quell'oggetto.

Quando si verifica una violazione della policy QoS condivisa, in questo campo viene visualizzato solo l'oggetto del carico di lavoro che consuma più IOPS o MB/s. I carichi di lavoro aggiuntivi che utilizzano questo criterio vengono visualizzati nella pagina Dettagli evento.

- **Tipo di fonte**

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 dell'evento**

Se l'evento ha avuto origine dal "Portale Active IQ " o direttamente da "Active IQ Unified Manager".

- **Nome dell'annotazione**

Nome dell'annotazione assegnata all'oggetto di archiviazione.

- **Note**

Numero di note aggiunte per un evento.

- **Giorni eccezionali**

Numero di giorni trascorsi dalla prima generazione dell'evento.

- **Tempo assegnato**

Tempo trascorso da quando l'evento è stato assegnato a un utente. Se il tempo trascorso supera una settimana, viene visualizzato il timestamp in cui l'evento è stato assegnato a un utente.

- **Riconosciuto da**

Il nome dell'utente che ha riconosciuto l'evento. Il campo è vuoto se l'evento non è riconosciuto.

- **Ora riconosciuta**

Il tempo trascorso da quando l'evento è stato riconosciuto. Se il tempo trascorso supera una settimana, viene visualizzato il timestamp in cui l'evento è stato riconosciuto.

- **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 visualizzato il timestamp in cui l'evento è stato risolto.

- **Tempo obsoleto**

Il momento 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, come la gravità dell'evento, il livello di impatto, l'area di impatto e l'origine dell'evento. È inoltre possibile visualizzare informazioni aggiuntive sulle possibili soluzioni per risolvere il problema.

- **Nome dell'evento**

Il nome dell'evento e l'ora in cui è stato visualizzato l'ultima volta.

Per gli eventi non performanti, mentre l'evento si trova nello stato Nuovo o Riconosciuto, le ultime informazioni visualizzate non sono note e pertanto sono nascoste.

- **Descrizione dell'evento**

Una breve descrizione dell'evento.

In alcuni casi, nella descrizione dell'evento viene specificato il motivo per cui l'evento è stato attivato.

- **Componente in lizza**

Per gli eventi di prestazioni dinamiche, questa sezione visualizza le icone che rappresentano i componenti

logici e fisici del cluster. Se un componente è in conflitto, la sua icona viene cerchiata ed evidenziata in rosso.

Per una descrizione dei componenti visualizzati qui, vedere *Componenti del cluster e perché possono essere in competizione*.

Le sezioni Informazioni sull'evento, Diagnosi di sistema e Azioni suggerite sono descritte in altri argomenti.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **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**

Ti assegna l'evento.

- **Assegna ad altri**

Apri 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 anche possibile annullare l'assegnazione degli eventi lasciando vuoto il campo della 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 riconosciuto l'evento vengono aggiunti all'elenco degli eventi (Riconosciuto da) per gli eventi selezionati. Quando riconosci un evento, ti assumi la responsabilità di gestirlo.

- **Segna come risolto**

Consente di modificare lo stato dell'evento in Risolto.

Quando risolvi un evento, il tuo nome utente e l'ora in cui hai risolto l'evento vengono aggiunti all'elenco degli eventi (Risolto da) per gli eventi selezionati. Dopo aver adottato misure correttive 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.

Cosa visualizza la sezione Informazioni sull'evento

Utilizzare la sezione Informazioni evento nella pagina Dettagli evento per visualizzare i dettagli relativi a un evento selezionato, ad esempio la gravità dell'evento, il livello di impatto, l'area di impatto e l'origine dell'evento.

I campi che non sono applicabili al tipo di evento sono nascosti. Puoi visualizzare i seguenti dettagli dell'evento:

- **Ora di attivazione dell'evento**

Ora in cui è stato generato l'evento.

- **Stato**

Stato dell'evento: Nuovo, Riconosciuto, Risolto o Obsoleto.

- **Causa obsoleta**

Le azioni che hanno causato l'obsolescenza dell'evento, ad esempio il problema è stato risolto.

- **Durata dell'evento**

Per gli eventi attivi (nuovi e riconosciuti), questo è il tempo che intercorre tra il rilevamento e l'ora in cui l'evento è stato analizzato per l'ultima volta. Per gli eventi obsoleti, questo è il tempo trascorso tra il rilevamento e la risoluzione dell'evento.

Questo campo viene visualizzato per tutti gli eventi di performance e per altri tipi di eventi solo dopo che sono stati risolti o resi obsoleti.

- **Ultimo avvistamento**

Data e ora in cui l'evento è stato visualizzato per l'ultima volta come attivo.

Per gli eventi di performance questo valore potrebbe essere più recente dell'ora di attivazione dell'evento, poiché questo campo viene aggiornato dopo ogni nuova raccolta di dati sulle performance, purché l'evento sia attivo. Per altri tipi di eventi, quando si trovano nello stato Nuovo o Riconosciuto, questo contenuto non viene aggiornato e il campo risulta quindi nascosto.

- **Gravità**

Gravità dell'evento: Critico (❌), Errore (⚠️), Avvertimento (⚠️), e Informazioni (ℹ️).

- **Livello di impatto**

Livello di impatto dell'evento: incidente, rischio, evento o aggiornamento.

- **Area di impatto**

Area di impatto dell'evento: disponibilità, capacità, prestazioni, protezione, configurazione o sicurezza.

- **Fonte**

Il nome dell'oggetto su cui si è verificato l'evento.

Quando si visualizzano i dettagli di un evento di policy QoS condiviso, in questo campo vengono elencati

fino a tre degli oggetti del carico di lavoro che consumano più IOPS o MBps.

È possibile fare clic sul collegamento del nome della sorgente per visualizzare la pagina dei dettagli sullo stato o sulle prestazioni di quell'oggetto.

- **Annotazioni sulla fonte**

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 fonte**

Tipo di oggetto (ad esempio, SVM, Volume o Qtree) a cui è associato l'evento.

- **Su Cluster**

Nome del cluster in cui si è verificato l'evento.

È possibile fare clic sul collegamento al nome del cluster per visualizzare la pagina dei dettagli sullo stato o sulle prestazioni di quel cluster.

- **Conteggio oggetti interessati**

Numero di oggetti interessati dall'evento.

È possibile fare clic sul collegamento dell'oggetto per visualizzare la pagina dell'inventario popolata con gli oggetti attualmente interessati da questo evento.

Questo campo viene visualizzato solo per gli eventi di performance.

- **Volumi interessati**

Numero di volumi interessati da questo evento.

Questo campo viene visualizzato solo per gli eventi di performance sui nodi o sugli aggregati.

- **Politica attivata**

Nome della policy di soglia che ha generato l'evento.

È possibile passare il cursore sul nome della policy per visualizzare i dettagli della policy di soglia. Per le policy QoS adattive vengono visualizzati anche la policy definita, la dimensione del blocco e il tipo di allocazione (spazio allocato o spazio utilizzato).

Questo campo viene visualizzato solo per gli eventi di performance.

- **ID regola**

Per gli eventi della piattaforma Active IQ , questo è il numero della regola che è stata attivata per generare

l'evento.

- **Riconosciuto da**

Il nome della persona che ha riconosciuto 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 a cui è assegnato il lavoro sull'evento.

- **Impostazioni di avviso**

Vengono visualizzate le seguenti informazioni sugli avvisi:

- Se non ci sono avvisi associati all'evento selezionato, viene visualizzato il collegamento **Aggiungi avviso**.

È possibile aprire la finestra di dialogo Aggiungi avviso facendo clic sul collegamento.

- Se all'evento selezionato è associato un avviso, viene visualizzato il nome dell'avviso.

È possibile aprire la finestra di dialogo Modifica avviso facendo clic sul collegamento.

- Se all'evento selezionato è associato più di un avviso, viene visualizzato il numero di avvisi.

È possibile aprire la pagina Impostazione avvisi facendo clic sul collegamento per visualizzare maggiori dettagli su questi avvisi.

Gli avvisi disattivati non vengono visualizzati.

- **Ultima notifica inviata**

Data e ora in cui è stata inviata la notifica di avviso più recente.

- **Invia tramite**

Il meccanismo utilizzato per inviare la notifica di avviso: e-mail o trap SNMP.

- **Esecuzione script precedente**

Nome dello script eseguito quando è stato generato l'avviso.

Cosa viene visualizzato nella sezione Azioni suggerite

La sezione Azioni suggerite della pagina dei dettagli dell'evento fornisce le possibili cause dell'evento e suggerisce alcune azioni in modo che tu possa provare a risolverlo autonomamente. Le azioni suggerite vengono personalizzate in base al tipo di evento o al tipo di soglia superata.

Quest'area viene visualizzata solo per alcuni tipi di eventi.

In alcuni casi nella pagina sono presenti link di **Aiuto** che rimandano a informazioni aggiuntive per molte azioni suggerite, tra cui istruzioni per eseguire un'azione specifica. Alcune azioni potrebbero comportare l'utilizzo di Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, comandi ONTAP CLI o una combinazione di questi strumenti.

Dovresti considerare le azioni suggerite qui solo come una guida per risolvere questo evento. L'azione da intraprendere per risolvere questo evento dovrebbe basarsi sul contesto del proprio ambiente.

Se si desidera analizzare l'oggetto e l'evento in modo più dettagliato, fare clic sul pulsante **Analizza carico di lavoro** per visualizzare la pagina Analisi carico di lavoro.

Ci sono alcuni eventi che Unified Manager può diagnosticare in modo approfondito e fornire una soluzione univoca. Se disponibili, tali risoluzioni vengono visualizzate con un pulsante **Correggi**. Fare clic su questo pulsante per far sì che Unified Manager risolva il problema che causa l'evento.

Per gli eventi della piattaforma Active IQ, questa sezione potrebbe contenere un collegamento a un articolo della Knowledgebase NetApp, se disponibile, che descrive il problema e le possibili soluzioni. Nei siti senza accesso alla rete esterna, un PDF dell'articolo della Knowledgebase viene aperto localmente; il PDF fa parte del file delle regole che si scarica manualmente nell'istanza di Unified Manager.

Cosa visualizza la sezione Diagnosi di sistema

La sezione Diagnosi di sistema della pagina Dettagli evento fornisce informazioni che possono aiutarti a diagnosticare i problemi che potrebbero essere stati la causa dell'evento.

Questa area viene visualizzata solo per alcuni eventi.

Alcuni eventi di performance forniscono grafici pertinenti all'evento specifico che è stato attivato. In genere include un grafico IOPS o MBps e un grafico della latenza per i dieci giorni precedenti. In questo modo è possibile vedere quali componenti di archiviazione incidono maggiormente sulla latenza o sono maggiormente interessati dalla latenza quando l'evento è attivo.

Per gli eventi di prestazioni dinamiche vengono visualizzati i seguenti grafici:

- Latenza del carico di lavoro: visualizza la cronologia della latenza per i carichi di lavoro principali di tipo vittima, bullo o squalo nel componente in competizione.
- Attività del carico di lavoro: visualizza i dettagli sull'utilizzo del carico di lavoro del componente del cluster in competizione.
- Attività delle risorse: visualizza le statistiche storiche sulle prestazioni del componente del cluster in competizione.

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 archiviazione. In alcuni casi saranno presenti una o più righe, una per ogni componente analizzato, per le policy di prestazione definite dal sistema che analizzano più contatori di prestazione. In questo scenario, accanto alla diagnosi viene visualizzata un'icona verde o rossa per indicare se è stato rilevato un problema o meno in quella particolare diagnosi.

Pagina di configurazione dell'evento

La pagina Configurazione evento visualizza l'elenco degli eventi disabilitati e fornisce

informazioni quali il tipo di oggetto associato e la gravità dell'evento. È anche possibile eseguire attività quali la disabilitazione o l'abilitazione di eventi a livello globale.

Puoi accedere a questa pagina solo se disponi del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per gli eventi selezionati:

- **Disabilita**

Avvia la finestra di dialogo Disabilita eventi, che puoi utilizzare per disabilitare gli eventi.

- **Abilitare**

Abilita gli eventi selezionati che avevi scelto di disabilitare in precedenza.

- **Regole di caricamento**

Avvia la finestra di dialogo Carica regole, che consente ai siti senza accesso alla rete esterna di caricare manualmente il file delle regole di Active IQ su Unified Manager. Le regole vengono eseguite sui messaggi AutoSupport del cluster per generare eventi per la configurazione del sistema, il cablaggio, le best practice e la disponibilità, come definito dalla piattaforma Active IQ .

- **Iscriviti agli eventi EMS**

Avvia 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 che si stanno monitorando. L'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 gravità appropriata.

Visualizzazione elenco

La vista Elenco mostra (in formato tabellare) le informazioni sugli eventi disabilitati. È possibile utilizzare i filtri delle colonne per personalizzare i dati visualizzati.

- **Evento**

Visualizza il nome dell'evento disabilitato.

- **Gravità**

Visualizza la gravità dell'evento. La gravità può essere Critica, Errore, Avviso o Informazione.

- **Tipo di fonte**

Visualizza il tipo di origine per cui viene generato l'evento.

Finestra di dialogo Disabilita eventi

Nella finestra di dialogo Disabilita eventi viene visualizzato l'elenco dei tipi di evento per i quali è possibile disabilitare gli eventi. È possibile disabilitare gli eventi per un tipo di evento in base a una particolare gravità o per un insieme di eventi.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Area Proprietà evento

L'area Proprietà evento specifica le seguenti proprietà dell'evento:

- **Gravità dell'evento**

Consente di selezionare gli eventi in base al tipo di gravità, che può essere Critico, Errore, Avviso o Informazione.

- **Il nome dell'evento contiene**

Consente di filtrare gli eventi il cui nome contiene i caratteri specificati.

- **Eventi corrispondenti**

Visualizza l'elenco degli eventi che corrispondono al tipo di gravità dell'evento e alla stringa di testo specificata.

- **Disabilita eventi**

Visualizza l'elenco degli eventi selezionati per la disattivazione.

Insieme al nome dell'evento viene visualizzata anche la gravità.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per gli eventi selezionati:

- **Salva e chiudi**

Disabilita il tipo di evento e chiude la finestra di dialogo.

- **Cancellare**

Annulla le modifiche e chiude la finestra di dialogo.

Gestisci gli avvisi

È possibile configurare gli avvisi in modo che vengano inviate notifiche automatiche quando si verificano eventi specifici o eventi di determinati tipi di gravità. È anche possibile associare un avviso a uno script che viene eseguito quando viene attivato un avviso.

Cosa sono gli avvisi

Sebbene gli eventi si verifichino continuamente, Unified Manager genera un avviso solo quando un evento soddisfa i criteri di filtro specificati. È possibile scegliere gli eventi per i quali generare avvisi, ad esempio quando viene superata una soglia di spazio o un oggetto va offline. È anche possibile associare un avviso a uno script che viene eseguito quando viene attivato un avviso.

I criteri di filtro includono la classe dell'oggetto, il nome o la gravità dell'evento.

Quali informazioni sono contenute in un'e-mail di avviso

Le email di avviso di Unified Manager forniscono il tipo di evento, la gravità dell'evento, il nome della policy o della soglia che è stata violata causando l'evento e una descrizione dell'evento. Il messaggio di posta elettronica fornisce anche 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 iscritti per ricevere gli avvisi.

Se un contatore delle prestazioni o un valore di capacità subisce una variazione significativa durante un periodo di raccolta, potrebbe causare l'attivazione contemporanea di un evento critico e di un evento di avviso per la stessa policy di soglia. In questo caso, potresti ricevere un'e-mail per l'evento di avviso e una per l'evento critico. Questo perché Unified Manager consente di abbonarsi separatamente per ricevere avvisi in caso di superamento delle soglie di attenzione e critiche.

Di seguito è riportato un esempio di e-mail di avviso:

From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclus@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>

Aggiungi avvisi

È possibile configurare degli avvisi per essere avvisati quando viene generato un evento specifico. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un tipo di gravità specifico. È possibile specificare la frequenza con

cui si desidera ricevere la notifica e associare uno script all'avviso.

Prima di iniziare

- È necessario aver configurato le impostazioni di notifica, quali l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP, per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento.
- 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 a cui si desidera inviare la notifica.
- Se si desidera che uno script venga eseguito in base all'evento, è necessario aver aggiunto lo script a Unified Manager tramite la pagina Script.
- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Impostazione avviso, come descritto qui.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina **Impostazione avviso**, fare clic su **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 **Il nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse che corrispondono alla regola del filtro. La stringa di testo specificata è sensibile alla distinzione tra maiuscole e minuscole.

Se una risorsa è conforme sia alle regole di inclusione che a quelle di 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 gravità dell'evento per cui si desidera attivare un avviso.



Per selezionare più di un evento, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **Azioni** e selezionare gli utenti a cui si desidera inviare la notifica, scegliere la frequenza della 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 email specificato per l'utente e si riapre l'avviso per modificarlo, il campo Nome appare vuoto perché l'indirizzo email modificato non è più associato all'utente precedentemente selezionato. Inoltre, se hai modificato l'indirizzo email dell'utente selezionato dalla pagina Utenti, l'indirizzo email modificato non verrà aggiornato per l'utente selezionato.

È anche possibile scegliere di avvisare gli utenti tramite trap SNMP.

7. Fare clic su **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 essere avvisato ogni 15 minuti

Eseguire i seguenti passaggi nella finestra di dialogo Aggiungi avviso:

1. Fai clic su **Nome** e inserisci `*HealthTest *` nel campo **Nome avviso**.
2. Fare clic su **Risorse** e, nella scheda Includi, selezionare **Volumi** dall'elenco a discesa.
 - a. Entra `*abc *` nel campo **Il nome contiene** per visualizzare i volumi il cui nome contiene "abc".
 - b. Seleziona **+ [All Volumes whose name contains 'abc'] +** dall'area Risorse disponibili e spostarlo nell'area Risorse selezionate.
 - c. Fai clic su **Escludi** e inserisci `*xyz *` nel campo **Il nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **Critico** dal campo Gravità evento.
4. Seleziona **Tutti gli eventi critici** dall'area Eventi corrispondenti e spostalo nell'area Eventi selezionati.
5. Fai clic su **Azioni** e inserisci `*sample@domain.com *` nel campo Avvisa questi utenti.
6. Seleziona **Ricorda ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

È possibile configurare un avviso in modo che invii ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario stabilire l'orario a partire dal quale la notifica dell'evento è attiva per l'avviso.

7. Nel menu Seleziona script da eseguire, seleziona script **Test**.
8. Fare clic su **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, e ad eventi di un tipo di gravità specifico. Come buona pratica, puoi aggiungere un avviso per uno qualsiasi degli oggetti critici dopo aver aggiunto il cluster a cui appartiene l'oggetto.

È possibile utilizzare le seguenti linee guida e considerazioni per creare avvisi e gestire i sistemi in modo efficace:

- Descrizione dell'avviso

Dovresti fornire una descrizione per l'avviso, in modo da aiutarti a monitorare efficacemente i tuoi avvisi.

- Risorse

Dovresti decidere quale risorsa fisica o logica richiede un avviso. È possibile includere ed escludere risorse, a seconda delle necessità. Ad esempio, se si desidera monitorare attentamente gli aggregati configurando un avviso, è necessario selezionare gli aggregati richiesti dall'elenco delle risorse.

Se selezioni una categoria di risorse, ad esempio **+[\[All User or Group Quotas\]](#)+**, riceverai avvisi per tutti gli oggetti in quella categoria.



La selezione di un cluster come risorsa non comporta la selezione automatica degli oggetti di archiviazione 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.

- **Gravità dell'evento**

È necessario decidere se un evento di un tipo di gravità specificato (critico, errore, avviso) debba attivare l'avviso e, in tal caso, quale tipo di gravità.

- **Eventi selezionati**

Se si aggiunge un avviso in base al tipo di evento generato, è necessario decidere quali eventi richiedono un avviso.

Se selezioni la gravità di un evento, ma non selezioni alcun evento individuale (se lasci vuota la colonna "Eventi selezionati"), riceverai avvisi per tutti gli eventi nella categoria.

- **Azioni**

È necessario fornire i nomi utente e gli indirizzi e-mail degli utenti che riceveranno la notifica. È anche possibile specificare una 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 di notifica**

È possibile configurare un avviso in modo che invii ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario stabilire l'orario a partire dal quale la notifica dell'evento è attiva per l'avviso. Se si desidera che la notifica dell'evento venga ripetuta finché l'evento non viene riconosciuto, è necessario stabilire la frequenza con cui si desidera che la notifica venga ripetuta.

- **Esegui script**

Puoi associare il tuo script a un avviso. Lo script viene eseguito quando viene generato l'avviso.

Aggiungi avvisi per eventi di performance

È possibile configurare avvisi per singoli eventi di prestazioni, proprio come per qualsiasi altro evento ricevuto da Unified Manager. Inoltre, se vuoi trattare tutti gli eventi di performance allo stesso modo e inviare un'e-mail alla stessa persona, puoi creare un singolo avviso per essere avvisato quando vengono attivati eventi di performance critici o di avvertenza.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

L'esempio seguente mostra come creare un evento per tutti gli eventi critici di latenza, IOPS e MBps. È possibile utilizzare la stessa metodologia per selezionare gli eventi da tutti i contatori delle prestazioni e per tutti gli eventi di avviso.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina **Impostazione avviso**, fare clic su **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 è selezionata alcuna risorsa, 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 azioni:
 - a. Nell'elenco Gravità evento, selezionare **Critico**.
 - b. Nel campo Il nome dell'evento contiene, immettere `*latency *` e quindi fare clic sulla freccia per selezionare tutti gli eventi corrispondenti.
 - c. Nel campo Il nome dell'evento contiene, immettere `*iops *` e quindi fare clic sulla freccia per selezionare tutti gli eventi corrispondenti.
 - d. Nel campo Il nome dell'evento contiene, immettere `*mbps *` e quindi fare clic sulla freccia per selezionare tutti gli eventi corrispondenti.
6. Fare clic su **Azioni** e quindi selezionare il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
7. Configurare qualsiasi altra opzione in questa pagina per l'emissione di trap SNMP e l'esecuzione di uno script.
8. Fare clic su **Salva**.

Avvisi di prova

Puoi testare un avviso per verificare di averlo configurato correttamente. Quando viene attivato un evento, viene generato un avviso e un'e-mail di avviso viene inviata ai destinatari configurati. È possibile verificare se la notifica è stata inviata e se lo script è stato eseguito utilizzando l'avviso di prova.

Prima di iniziare

- È necessario aver configurato le impostazioni di notifica, quali l'indirizzo e-mail dei destinatari, il server SMTP e la 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 in modo che venga eseguito quando viene generato l'avviso.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina **Impostazione avviso**, seleziona l'avviso che vuoi testare, quindi fai clic su **Test**.

Un'e-mail di avviso di prova verrà inviata agli indirizzi e-mail specificati durante la creazione dell'avviso.

Abilita e disabilita gli 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, Riconosciuto, Risolto e Obsoleto. Se non si desidera ricevere avvisi per gli eventi che passano agli stati Risolto e Obsoleto, è possibile configurare un'impostazione globale per sopprimere tali avvisi.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per impostazione predefinita, gli avvisi non vengono inviati per gli eventi quando passano agli stati Risolto e Obsoleto.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina **Impostazione avvisi**, eseguire una delle seguenti azioni utilizzando il controllo cursore accanto alla voce **Avvisi per eventi risolti e obsoleti**:

A...	Fai questo...
Interrompere l'invio di avvisi quando gli eventi vengono risolti o diventano obsoleti	Spostare il controllo del cursore verso sinistra
Inizia a inviare avvisi quando gli eventi vengono risolti o diventano obsoleti	Spostare il controllo del cursore verso destra

Escludere i volumi di destinazione del ripristino di emergenza dalla generazione di avvisi

Quando si configurano gli avvisi sui volumi, 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 ripristino di emergenza per le SVM, i volumi di origine e di destinazione hanno lo stesso nome, quindi si riceveranno avvisi per entrambi i volumi.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile disabilitare gli avvisi per i volumi di destinazione del ripristino di emergenza escludendo i volumi che hanno lo stesso nome dell'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 escludere la generazione dell'avviso su un volume con lo stesso nome sulla SVM "vs1-dr".

Eseguire i seguenti passaggi nella finestra di dialogo Aggiungi avviso:

Passi

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 immettere `*vol1 *` nel campo **Il nome contiene** per visualizzare i volumi il cui nome contiene "vol1".
 - b. Seleziona **+[\[All Volumes whose name contains 'vol1'\]](#) +** dall'area **Risorse disponibili** e spostarlo nell'area **Risorse selezionate**.
3. Selezionare la scheda **Escludi**, selezionare **Volume**, immettere `*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** e quindi selezionare il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
6. Configurare eventuali altre opzioni in questa pagina per l'emissione di trap SNMP e l'esecuzione di uno script, quindi fare clic su **Salva**.

Visualizza avvisi

È possibile visualizzare l'elenco degli avvisi creati per vari eventi dalla pagina Configurazione avvisi. È inoltre possibile visualizzare le proprietà dell'avviso, ad esempio la descrizione dell'avviso, il metodo e la frequenza di notifica, gli eventi che attivano l'avviso, i destinatari e-mail degli avvisi e le risorse interessate, ad esempio cluster, aggregati e volumi.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Fare un passo

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.

L'elenco degli avvisi viene visualizzato nella pagina Impostazione avvisi.

Modifica avvisi

È possibile modificare le proprietà dell'avviso, ad esempio la risorsa a cui è associato l'avviso, gli eventi, i destinatari, le opzioni di notifica, la frequenza di notifica e gli script associati.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina **Impostazione avviso**, seleziona l'avviso che desideri modificare e fai clic su **Modifica**.
3. Nella finestra di dialogo **Modifica avviso**, modifica le sezioni nome, risorse, eventi e azioni, come richiesto.

È possibile modificare o rimuovere lo script associato all'avviso.

4. Fare clic su **Salva**.

Elimina avvisi

È possibile eliminare un avviso quando non è più necessario. Ad esempio, è possibile eliminare un avviso creato per una risorsa specifica quando tale risorsa non è più monitorata da Unified Manager.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina **Impostazione avvisi**, seleziona gli avvisi che desideri eliminare e fai 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 per ricevere notifiche sugli eventi utilizzando la finestra di dialogo **Aggiungi avviso**. È anche possibile visualizzare l'elenco degli avvisi dalla pagina **Impostazione avvisi**.

Pagina di configurazione degli avvisi

La pagina **Impostazione avvisi** visualizza un elenco di avvisi e fornisce informazioni sul nome dell'avviso, sullo stato, sul metodo di notifica e sulla frequenza di notifica. Da questa pagina puoi anche aggiungere, modificare, rimuovere, abilitare o disabilitare gli avvisi.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Pulsanti di comando

- **Aggiungere**

Visualizza la finestra di dialogo **Aggiungi avviso**, che consente di aggiungere nuovi avvisi.

- **Modificare**

Visualizza la finestra di dialogo **Modifica avviso**, che consente di modificare gli avvisi selezionati.

- **Eliminare**

Elimina gli avvisi selezionati.

- **Abilitare**

Abilita gli avvisi selezionati a inviare notifiche.

- **Disabilita**

Disattiva gli avvisi selezionati quando si desidera interrompere temporaneamente l'invio delle notifiche.

- **Test**

Esegue il test degli avvisi selezionati per verificarne la configurazione dopo essere stati aggiunti o modificati.

- **Avvisi per eventi risolti e obsoleti**

Consente di abilitare o disabilitare l'invio di avvisi quando gli eventi vengono spostati negli stati Risolto o Obsoleto. Ciò può impedire agli utenti di ricevere notifiche non necessarie.

Visualizzazione elenco

La vista elenco mostra, in formato tabellare, le informazioni sugli avvisi creati. È possibile utilizzare i filtri delle colonne per personalizzare i dati visualizzati. Puoi anche selezionare un avviso per visualizzare maggiori informazioni nell'area dettagli.

- **Stato**

Specifica se un avviso è abilitato () o disabilitato () .

- **Attenzione**

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 avvisare gli utenti tramite e-mail o trap SNMP.

- **Frequenza di notifica**

Specifica la frequenza (in minuti) con cui il server di gestione continua a inviare notifiche finché l'evento non viene riconosciuto, risolto o spostato nello stato Obsoleto.

Area dettagli

L'area dei dettagli fornisce maggiori informazioni sull'avviso selezionato.

- **Nome avviso**

Visualizza il nome dell'avviso.

- **Descrizione dell'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.

- **Esclude**

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 finché l'evento non viene riconosciuto, risolto o spostato nello stato Obsoleto.

- **Nome dello script**

Visualizza il nome dello script associato all'avviso selezionato. Questo script viene eseguito quando viene generato un avviso.

- **Destinatari e-mail**

Visualizza gli indirizzi email degli utenti che ricevono la notifica di avviso.

Finestra di dialogo Aggiungi avviso

È possibile creare avvisi per essere avvisati quando viene generato un evento specifico, 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 per un insieme di risorse e per eventi di un tipo di gravità specifico. È inoltre possibile specificare il metodo di notifica e la frequenza degli avvisi.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Nome

Quest'area consente di specificare un nome e una descrizione per l'avviso:

- **Nome avviso**

Consente di specificare un nome per l'avviso.

- **Descrizione dell'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 risorse selezionando un tipo di risorsa dall'elenco a discesa oppure è possibile specificare il nome esatto della risorsa per visualizzarne una specifica.

Se si crea un avviso da una qualsiasi delle pagine dei dettagli dell'oggetto di archiviazione, l'oggetto di archiviazione viene automaticamente incluso nell'avviso.

- **Includere**

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".

- **Escludere**

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 selezioni tutte le risorse di un particolare tipo di risorsa: ad esempio, [+\[All Volumes\]](#) O [+\[All Volumes whose name contains 'xyz'\]](#) +.

Se una risorsa è conforme sia alle regole di inclusione che a quelle di esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per l'evento.

Eventi

In questa area è possibile selezionare gli eventi per i quali si desidera creare gli avvisi. È possibile creare avvisi per eventi in base a una particolare gravità o per un insieme di eventi.

Per selezionare più di un evento, tieni premuto il tasto Ctrl mentre effettui le selezioni.

- **Gravità dell'evento**

Consente di selezionare gli eventi in base al tipo di gravità, 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

In questa area è possibile specificare gli utenti a cui inviare una notifica quando viene attivato un avviso. È inoltre possibile specificare il metodo di notifica e la frequenza della notifica.

- **Avvisa questi utenti**

Consente di specificare l'indirizzo email o il nome utente dell'utente che riceverà le notifiche.

Se si modifica l'indirizzo email specificato per l'utente e si riapre l'avviso per modificarlo, il campo Nome appare vuoto perché l'indirizzo email modificato non è più associato all'utente precedentemente selezionato. Inoltre, se hai modificato l'indirizzo email dell'utente selezionato dalla pagina Utenti, l'indirizzo

email modificato non verrà aggiornato per l'utente selezionato.

- **Frequenza di notifica**

Consente di specificare la frequenza con cui il server di gestione invia notifiche finché l'evento non viene riconosciuto, risolto o spostato nello stato obsoleto.

Puoi scegliere i seguenti metodi di notifica:

- Notificare solo una volta
- Notificare con una frequenza specificata
- Notificare con una frequenza specificata entro l'intervallo di tempo specificato

- **Emetti trap SNMP**

Selezionando questa casella è possibile specificare se le trap SNMP devono essere inviate all'host SNMP configurato globalmente.

- **Esegui script**

Consente di aggiungere il proprio script personalizzato all'avviso. Questo script viene eseguito quando viene generato un avviso.



Se questa funzionalità non è disponibile nell'interfaccia utente, è perché è stata disabilitata dall'amministratore. Se necessario, è possibile abilitare questa funzionalità da **Gestione archiviazione > Impostazioni funzionalità**.

Pulsanti di comando

- **Salva**

Crea un avviso e chiude la finestra di dialogo.

- **Cancellare**

Annulla le modifiche e chiude la finestra di dialogo.

Finestra di dialogo Modifica avviso

È possibile modificare le proprietà dell'avviso, ad esempio la risorsa a cui è associato, gli eventi, lo 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 dell'avviso**

Consente di specificare una descrizione per l'avviso.

- **Stato di allerta**

Consente di abilitare o disabilitare 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 risorse selezionando un tipo di risorsa dall'elenco a discesa oppure è possibile specificare il nome esatto della risorsa per visualizzarne una specifica.

- **Includere**

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".

- **Escludere**

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 selezioni tutte le risorse di un particolare tipo di risorsa, ad esempio [+\[All Volumes\]](#) + o [+\[All Volumes whose name contains 'xyz'\]](#) +.

Eventi

In questa area è possibile selezionare gli eventi per i quali si desidera attivare gli avvisi. È possibile attivare un avviso per eventi basati su una particolare gravità o per una serie di eventi.

- **Gravità dell'evento**

Consente di selezionare gli eventi in base al tipo di gravità, 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

In questa area è possibile specificare il metodo di notifica e la frequenza della notifica.

- **Avvisa questi utenti**

Consente di modificare l'indirizzo email o il nome utente oppure di specificare un nuovo indirizzo email o nome utente per ricevere le notifiche.

- **Frequenza di notifica**

Consente di modificare la frequenza con cui il server di gestione invia notifiche finché l'evento non viene riconosciuto, risolto o spostato nello stato obsoleto.

Puoi scegliere i seguenti metodi di notifica:

- Notificare solo una volta
- Notificare con una frequenza specificata
- Notificare con una frequenza specificata entro l'intervallo di tempo specificato

- **Emetti trap SNMP**

Consente di specificare se le trap SNMP devono essere inviate all'host SNMP configurato globalmente.

- **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.

- **Cancellare**

Annulla le modifiche e chiude la finestra di dialogo.

Gestisci gli script

È possibile utilizzare gli script per modificare o aggiornare automaticamente più oggetti di archiviazione 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.

La possibilità di caricare script su Unified Manager ed eseguirli è abilitata per impostazione predefinita. Se la tua organizzazione non desidera consentire questa funzionalità per motivi di sicurezza, puoi disattivarla da **Gestione archiviazione > Impostazioni funzionalità**.

Informazioni correlate

["Abilitazione e disabilitazione della possibilità di caricare 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 problemi con gli oggetti di archiviazione o identificare quali oggetti di archiviazione generano gli eventi.

Quando viene generato un avviso per un evento in Unified Manager, viene inviata un'e-mail di avviso ai destinatari specificati. Se hai 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 hai creato uno script personalizzato e lo hai 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 **Correggi** non sono disponibili per impostazione predefinita nella pagina 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 sugli eventi correlati o modificare gli oggetti di archiviazione.

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`
```

Aggiungi 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 archiviazione per i quali viene generato l'evento.

Prima di iniziare

- 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

Piattaforma su cui è installato Unified Manager	Lingue supportate
Linux	Script Perl, Python e Shell
Finestre	Script PowerShell, Perl, Python e .bat

- Per gli script Perl, Perl deve essere installato sul server Unified Manager. Per le installazioni VMware, Perl 5 è installato per impostazione predefinita e gli script supporteranno solo ciò che Perl 5 supporta. Se Perl è stato installato dopo Unified Manager, è necessario riavviare il server Unified Manager.
- Per gli script di PowerShell, è necessario impostare sul server Windows i criteri di esecuzione di PowerShell appropriati affinché gli script possano essere eseguiti.



Se lo script crea file di registro per monitorare l'avanzamento dello script di avviso, è necessario assicurarsi che i file di registro non vengano creati in alcun punto della cartella di installazione di Unified Manager.

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile caricare script personalizzati e raccogliere dettagli sugli eventi relativi all'avviso.



Se questa funzionalità non è disponibile nell'interfaccia utente, è perché è stata disabilitata dall'amministratore. Se necessario, è possibile abilitare questa funzionalità da **Gestione archiviazione > Impostazioni funzionalità**.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Script**.
2. Nella pagina **Script**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi script**, fare clic su **Sfoglia** per selezionare il file di script.
4. Inserisci una descrizione per lo script selezionato.
5. Fare clic su **Aggiungi**.

Informazioni correlate

["Abilitazione e disabilitazione della possibilità di caricare script"](#)

Elimina gli script

È possibile eliminare uno script da Unified Manager quando non è più necessario o valido.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Lo script non deve essere associato a un avviso.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Script**.
2. Nella pagina **Script**, seleziona lo script che vuoi eliminare, quindi fai clic su **Elimina**.

3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Esecuzione dello script di test

È possibile verificare che lo script venga eseguito correttamente quando viene generato un avviso per un oggetto di archiviazione.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver caricato uno script nel formato di file supportato su Unified Manager.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Script**.
2. Nella pagina **Script**, aggiungi il tuo script di prova.
3. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
4. Nella pagina **Impostazione avviso**, eseguire una delle seguenti azioni:

A...	Fai questo...
Aggiungi un avviso	a. Fare clic su Aggiungi. b. Nella sezione Azioni, associa l'avviso allo script di test.
Modifica un avviso	a. Seleziona un avviso, quindi fai clic su Modifica. b. Nella sezione Azioni, associa l'avviso allo script di test.

5. Fare clic su **Salva**.
6. Nella pagina **Impostazione avviso**, seleziona l'avviso che hai aggiunto o modificato, quindi fai clic su **Test**.

Lo script viene eseguito con l'argomento "-test" e un avviso di notifica viene inviato agli indirizzi e-mail specificati al momento della creazione dell'avviso.

Comandi CLI di Unified Manager supportati

In qualità di amministratore di storage, puoi utilizzare i comandi CLI per eseguire query sugli oggetti di storage, ad esempio su cluster, aggregati, volumi, qtree e LUN. È possibile utilizzare i comandi CLI per interrogare il database interno di Unified Manager e il database ONTAP. È anche possibile utilizzare i comandi CLI negli script che vengono eseguiti all'inizio o alla fine di un'operazione oppure 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`, assicurati che il tuo account abbia accesso all'applicazione *console*.

comando CLI	Descrizione	Produzione
um cli login -u <username> [-p <password>]	Accede alla CLI. Per motivi di sicurezza, è opportuno immettere solo il nome utente dopo l'opzione "-u". Se utilizzato in questo modo, verrà richiesta la password, che non verrà memorizzata nella cronologia o nella tabella dei processi. La sessione scade dopo tre ore dal momento dell'accesso, dopodiché l'utente dovrà effettuare nuovamente l'accesso.	Visualizza il messaggio corrispondente.
um cli logout	Esce 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 gli script di avviso per ottenere o eseguire un'operazione su ONTAP. L'argomento facoltativo timeout imposta un limite di tempo massimo (in secondi) per il completamento del comando sul client. Il valore predefinito è 0 (attendi per sempre).	Come ricevuto da ONTAP.
um run query <sql command>	Esegue una query SQL. Sono consentite solo le query che leggono dal database. Non sono supportate operazioni di aggiornamento, inserimento o eliminazione.	I risultati vengono visualizzati in forma tabellare. Se viene restituito un set vuoto, oppure se si verifica un errore di sintassi o una richiesta errata, viene visualizzato il messaggio di errore appropriato.

comando CLI	Descrizione	Produzione
um datasource add -u <username> -P <password> [-t <protocol>] [-p <port>] <hostname-or-ip>	Aggiunge un'origine dati all'elenco dei sistemi di archiviazione gestiti. Un'origine dati descrive come vengono effettuate le connessioni ai sistemi di archiviazione. 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 è specificato, verranno tentati entrambi i protocolli. L'opzione -p (porta) specifica la porta utilizzata per comunicare con il cluster. Se la porta non viene specificata, verrà tentato il valore predefinito del protocollo appropriato. Questo comando può essere eseguito solo dall'amministratore dell'archiviazione.	Richiede all'utente di accettare il certificato e stampa il messaggio corrispondente.
um datasource list [<datasource-id>]	Visualizza le origini dati per i sistemi di archiviazione gestiti.	Visualizza i seguenti valori in formato tabellare: 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 dell'origine dati. Può essere eseguito solo dall'amministratore dell'archiviazione.	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 tabellare: Name, Value, Default Value, and Requires Restart.

comando CLI	Descrizione	Produzione
<code>um option set <option-name>=<option-value> [<option-name>=<option-value> ...]</code>	Imposta una o più opzioni. Il comando può essere eseguito solo dall'amministratore dell'archiviazione.	Visualizza il messaggio corrispondente.
<code>um version</code>	Visualizza la versione del software Unified Manager.	<code>Version ("9.6")</code>
<code>um lun list [-q] [-ObjectType <object-id>]</code>	Elenca i LUN dopo il filtraggio sull'oggetto specificato. -q è applicabile a tutti i comandi per non mostrare alcuna intestazione. ObjectType può essere lun, qtree, cluster, volume, quota o svm. Per esempio: um lun list -cluster 1 In questo esempio, "-cluster" è objectType e "1" è objectId. Il comando elenca tutti i LUN all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabellare: ID and LUN path.
<code>um svm list [-q] [-ObjectType <object-id>]</code>	Elenca le VM di archiviazione dopo aver filtrato l'oggetto specificato. ObjectType può essere lun, qtree, cluster, volume, quota o svm. Per esempio: um svm list -cluster 1 In questo esempio, "-cluster" è objectType e "1" è objectId. Il comando elenca tutte le VM di archiviazione all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabellare: Name and Cluster ID.

comando CLI	Descrizione	Produzione
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 mostrare alcuna intestazione. ObjectType può essere lun, qtree, cluster, volume, quota o svm. Per 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 tabellare: Qtree ID and Qtree Name.
um disk list [-q] [-ObjectType <object-id>]	Elenca i dischi dopo il filtraggio in base all'oggetto specificato. ObjectType può essere disk, aggr, node o cluster. Per 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 tabellare ObjectType and object-id.
um cluster list [-q] [-ObjectType <object-id>]	Elenca i cluster dopo il filtraggio in base all'oggetto specificato. ObjectType può essere disk, aggr, node, cluster, lun, qtree, volume, quota o svm. Per 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 tabellare: Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.

comando CLI	Descrizione	Produzione
<pre>um cluster node list [-q] [-ObjectType <object-id>]</pre>	Elenca i nodi del cluster dopo il filtraggio in base all'oggetto specificato. ObjectType può essere disk, aggr, node o cluster. Per esempio: <pre>um cluster node list -cluster 1</pre> 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 tabellare Name and Cluster ID.
<pre>um volume list [-q] [-ObjectType <object-id>]</pre>	Elenca i volumi dopo il filtraggio in base all'oggetto specificato. ObjectType può essere lun, qtree, cluster, volume, quota, svm o aggregate. Per esempio: <pre>um volume list -cluster 1</pre> 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 tabellare Volume ID and Volume Name.
<pre>um quota user list [-q] [-ObjectType <object-id>]</pre>	Elenca gli utenti con quota dopo aver filtrato l'oggetto specificato. ObjectType può essere qtree, cluster, volume, quota o svm. Per esempio: <pre>um quota user list -cluster 1</pre> In questo esempio, "-cluster" è objectType e "1" è objectId. Il comando elenca tutti gli utenti quota all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabellare ID, Name, SID and Email.

comando CLI	Descrizione	Produzione
<code>um aggr list [-q] [-ObjectType <object-id>]</code>	Elenca gli aggregati dopo il filtraggio in base all'oggetto specificato. ObjectType può essere disk, aggr, node, cluster o volume. Per 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 tabellare Aggr ID, and Aggr Name .
<code>um event ack <event-ids></code>	Riconosce uno o più eventi.	Visualizza il messaggio corrispondente.
<code>um event resolve <event-ids></code>	Risolve uno o più eventi.	Visualizza il messaggio corrispondente.
<code>um event assign -u <username> <event-id></code>	Assegna un evento a un utente.	Visualizza il messaggio corrispondente.
<code>um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]</code>	Elenca gli eventi generati dal sistema o dall'utente. Filtra gli eventi in base a origine, stato e ID.	Visualizza i seguenti valori in formato tabellare Source, Source type, Name, Severity, State, User and Timestamp .
<code>um backup restore -f <backup_file_path_and_name></code>	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 script personalizzati a Unified Manager. È possibile associare questi script agli avvisi per abilitare la riconfigurazione automatica degli oggetti di archiviazione.

La pagina Script consente di aggiungere o eliminare script da Unified Manager.

Pulsanti di comando

- **Aggiungere**

Visualizza la finestra di dialogo Aggiungi script, che consente di aggiungere script.

- **Eliminare**

Elimina lo script selezionato.

Visualizzazione elenco

La visualizzazione elenco mostra, in formato tabellare, gli script aggiunti a Unified Manager.

- **Nome**

Visualizza il nome dello script.

- **Descrizione**

Visualizza la descrizione dello script.

Finestra di dialogo 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 archiviazione.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

- **Seleziona file script**

Consente di selezionare uno script per l'avviso.

- **Descrizione**

Consente di specificare una descrizione per lo script.

Monitorare e gestire le prestazioni del cluster

Introduzione al monitoraggio delle prestazioni Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) offre funzionalità di monitoraggio delle prestazioni 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 utilizzano eccessivamente i componenti del cluster e riducono le prestazioni degli altri carichi di lavoro sul cluster. Definendo criteri di soglia delle prestazioni è anche possibile specificare valori massimi per determinati contatori delle prestazioni, in modo che vengano generati eventi quando la soglia viene superata. Unified Manager ti avvisa di questi eventi relativi alle prestazioni, in modo che tu possa adottare misure correttive e riportare le prestazioni ai normali livelli operativi. È possibile visualizzare e analizzare gli eventi nell'interfaccia utente di Unified Manager.

Unified Manager monitora le prestazioni 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 prestazioni di Unified Manager

Unified Manager raccoglie e analizza le statistiche sulle prestazioni dei sistemi che eseguono il software ONTAP . Utilizza soglie di prestazioni dinamiche e soglie di prestazioni definite dall'utente per monitorare una serie di contatori di prestazioni su numerosi componenti del cluster.

Un tempo di risposta elevato (latenza) indica che l'oggetto di archiviazione, ad esempio un volume, è più lento del normale. Questo problema indica anche che le prestazioni sono diminuite per le applicazioni client che utilizzano il volume. Unified Manager identifica il componente di archiviazione in cui si verifica il problema di prestazioni e fornisce un elenco di azioni suggerite che è possibile intraprendere per risolvere il problema.

Unified Manager include le seguenti funzionalità:

- Monitora e analizza le statistiche sulle prestazioni del carico di lavoro da un sistema che esegue il software ONTAP .
- Tiene traccia dei contatori delle prestazioni per cluster, nodi, aggregati, porte, SVM, volumi, LUN, namespace NVMe e interfacce di rete (LIF).
- Visualizza grafici dettagliati che tracciano l'attività del carico di lavoro nel tempo, inclusi IOPS (operazioni), MB/s (throughput), latenza (tempo di risposta), utilizzo, capacità delle prestazioni e rapporto della cache.
- Consente di creare criteri di soglia delle prestazioni definiti dall'utente che attivano eventi e inviano avvisi tramite e-mail quando le soglie vengono superate.
- Utilizza soglie definite dal sistema e soglie di prestazioni dinamiche che apprendono l'attività del carico di

lavoro per identificare e avvisare l'utente di eventuali problemi di prestazioni.

- Identifica le policy di qualità del servizio (QoS) e le policy di livello di servizio delle prestazioni (PSL) applicate ai volumi e alle LUN.
- Identifica chiaramente il componente del cluster in competizione.
- Identifica i carichi di lavoro che utilizzano eccessivamente i componenti del cluster e i carichi di lavoro le cui prestazioni sono influenzate dall'aumento dell'attività.

Interfacce Unified Manager utilizzate per gestire le prestazioni del sistema di archiviazione

Queste sezioni contengono informazioni sulle due interfacce utente fornite da Active IQ Unified Manager per la risoluzione dei problemi relativi alla capacità di archiviazione dei dati, alla disponibilità e alla protezione. Le due interfacce utente sono l'interfaccia utente Web di Unified Manager e la console di manutenzione.

Se si desidera utilizzare le funzionalità di protezione in Unified Manager, è necessario installare e configurare anche OnCommand Workflow Automation (WFA).

Interfaccia utente web di Unified Manager

L'interfaccia utente Web di Unified Manager consente all'amministratore di monitorare e risolvere i problemi del cluster relativi alla capacità di archiviazione dei dati, alla disponibilità e alla protezione.

In queste sezioni vengono descritti alcuni flussi di lavoro comuni che un amministratore può seguire per risolvere i problemi di capacità di archiviazione, 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 problemi del sistema operativo, problemi di aggiornamento della versione, problemi di accesso degli utenti e problemi di rete correlati 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 utilizzarle per risolvere i problemi relativi al funzionamento del server Unified Manager.

Attività di raccolta dati sulla configurazione e sulle prestazioni del cluster

L'intervallo di raccolta per i *dati di configurazione del cluster* è di 15 minuti. Ad esempio, dopo aver aggiunto un cluster, ci vogliono 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 verranno visualizzati nell'interfaccia utente dopo il successivo intervallo di polling, che potrebbe durare fino a 15 minuti.

Unified Manager raccoglie le statistiche sulle prestazioni correnti da tutti i cluster monitorati ogni cinque minuti. Analizza questi dati per identificare eventi prestazionali e potenziali problemi. Conserva 30 giorni di dati storici sulle prestazioni di cinque minuti e 180 giorni di dati storici sulle prestazioni di un'ora. Ciò consente di visualizzare dettagli molto granulari sulle prestazioni per il mese corrente e tendenze generali delle prestazioni

fino a un anno.

I sondaggi di raccolta vengono sfalsati di alcuni minuti in modo che i dati di ogni cluster non vengano inviati contemporaneamente, il che potrebbe influire sulle prestazioni.

Nella tabella seguente vengono descritte le attività di raccolta eseguite da Unified Manager:

Attività	Intervallo di tempo	Descrizione
Sondaggio sulle statistiche delle prestazioni	Ogni 5 minuti	Raccoglie dati sulle prestazioni in tempo reale da ciascun cluster.
Analisi statistica	Ogni 5 minuti	Dopo ogni sondaggio statistico, Unified Manager confronta i dati raccolti con soglie definite dall'utente, definite dal sistema e dinamiche. Se vengono superate le soglie di prestazione, Unified Manager genera eventi e invia e-mail agli utenti specificati, se configurato per farlo.
Sondaggio di configurazione	Ogni 15 minuti	Raccoglie informazioni di inventario dettagliate da ciascun cluster per identificare tutti gli oggetti di archiviazione (nodi, SVM, volumi e così via).
Riassunto	Ogni ora	Riassume le ultime 12 raccolte di dati sulle prestazioni di cinque minuti in medie orarie. I valori medi orari vengono utilizzati in alcune pagine dell'interfaccia utente e conservati per 180 giorni.
Analisi delle previsioni e potatura dei dati	Ogni giorno dopo mezzanotte	Analizza i dati del cluster per stabilire soglie dinamiche per la latenza del volume e gli IOPS per le successive 24 ore. Elimina dal database tutti i dati sulle prestazioni di cinque minuti più vecchi di 30 giorni.
Potatura dei dati	Ogni giorno 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.

Attività	Intervallo di tempo	Descrizione
Potatura dei dati	Tutti i giorni dopo le 3:30 del mattino	Elimina dal database tutti i dati sulle prestazioni orarie più vecchi di 180 giorni.

Cos'è un ciclo di raccolta della continuità dei dati

Un ciclo di raccolta della continuità dei dati recupera i dati sulle prestazioni al di fuori del ciclo di raccolta delle prestazioni 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 nei dati statistici che si verificano quando non è stato possibile raccogliere dati in tempo reale.

Unified Manager esegue sondaggi di raccolta della continuità dei dati sui dati storici delle prestazioni quando si verificano i seguenti eventi:

- Inizialmente un cluster viene aggiunto a Unified Manager.

Unified Manager raccoglie i dati storici sulle prestazioni dei 15 giorni precedenti. Ciò consente di visualizzare due settimane di informazioni sulle prestazioni storiche di un cluster, poche ore dopo la sua aggiunta.

Inoltre, se presenti, vengono segnalati gli eventi soglia definiti dal sistema per il periodo precedente.

- L'attuale ciclo di raccolta dei dati sulle prestazioni non si conclude nei tempi previsti.

Se il sondaggio sulle prestazioni in tempo reale supera il periodo di raccolta di cinque minuti, viene avviato un ciclo di raccolta di continuità dei dati per raccogliere le informazioni mancanti. Senza la raccolta di continuità dei dati, il periodo di raccolta successivo viene saltato.

- Unified Manager è stato inaccessibile per un certo periodo di tempo e poi è tornato online, come nelle seguenti situazioni:
 - È stato riavviato.
 - Si è spento durante un aggiornamento 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 poi torna online, come nelle seguenti situazioni:
 - Un'interruzione di rete viene riparata.
 - Una connessione di rete WAN lenta ha ritardato la normale raccolta dei dati sulle prestazioni.

Un ciclo di raccolta di continuità dei dati può raccogliere un massimo di 24 ore di dati storici. Se Unified Manager non è attivo per più di 24 ore, nelle pagine dell'interfaccia utente viene visualizzata una lacuna nei dati sulle prestazioni.

Un ciclo di raccolta di continuità dei dati e un ciclo di raccolta di dati in tempo reale non possono essere eseguiti contemporaneamente. Il ciclo di raccolta della continuità dei dati deve concludersi prima che venga avviata la raccolta dei dati sulle prestazioni 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

Il timestamp che appare nei dati raccolti su salute e prestazioni, o che appare come ora di rilevamento di un evento, si basa sull'ora del cluster ONTAP , adattata al fuso orario impostato sul 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 noti timestamp che sembrano errati per un cluster specifico, potresti voler verificare che l'ora del cluster sia stata impostata correttamente.

Esplora i flussi di lavoro delle prestazioni nell'interfaccia utente grafica di Unified Manager

L'interfaccia di Unified Manager fornisce numerose pagine per la raccolta e la visualizzazione delle informazioni sulle prestazioni. Per navigare tra le pagine dell'interfaccia utente grafica si utilizza il pannello di navigazione a sinistra, mentre per visualizzare e configurare le informazioni si utilizzano schede e collegamenti nelle pagine.

È possibile utilizzare tutte le seguenti pagine per monitorare e risolvere i problemi relativi alle informazioni sulle prestazioni del cluster:

- pagina del dashboard
- pagine di inventario degli oggetti di rete e di archiviazione
- pagine dei dettagli degli oggetti di archiviazione (incluso Performance Explorer)
- pagine di configurazione e impostazione
- pagine di eventi

Accedi all'interfaccia utente

È possibile accedere all'interfaccia utente di Unified Manager utilizzando un browser Web supportato.

Prima di iniziare

- Il browser web deve soddisfare i requisiti minimi.

Vedere la matrice di interoperabilità su ["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix) per l'elenco completo delle versioni dei browser supportate.

- È necessario disporre dell'indirizzo IP o dell'URL del server Unified Manager.

Verrai disconnesso automaticamente dalla sessione dopo 1 ora di inattività. Questo intervallo di tempo può essere configurato in **Generale > Impostazioni funzionalità**.

Passi

1. Inserisci l'URL nel tuo browser web, dove URL è l'indirizzo IP o il nome di dominio completo (FQDN) 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 accettare il rischio di continuare l'accesso oppure installare un certificato digitale firmato da un'autorità di certificazione (CA) per l'autenticazione del server. . Nella schermata di accesso, inserisci il tuo nome utente e la password.

Se l'accesso all'interfaccia utente di Unified Manager è protetto tramite autenticazione SAML, dovrai immettere le tue credenziali nella pagina di accesso del provider di identità (IdP) anziché nella pagina di accesso di Unified Manager.

Viene visualizzata la pagina Dashboard.



Se il server Unified Manager non è inizializzato, una nuova finestra del browser visualizza la prima procedura guidata. È necessario 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 a inviare informazioni sull'installazione di Unified Manager al supporto tecnico. Dopo aver completato queste informazioni, verrà visualizzata l'interfaccia utente di Unified Manager.

Interfaccia grafica e percorsi di navigazione

Unified Manager offre una grande flessibilità e consente di svolgere più attività in vari modi. Sono molti i percorsi di navigazione che scoprirai lavorando in Unified Manager. Sebbene non siano mostrate tutte le possibili combinazioni di navigazione, dovresti avere familiarità con alcuni degli scenari più comuni.

Monitorare la navigazione degli oggetti del cluster

È possibile monitorare le prestazioni di tutti gli oggetti in qualsiasi cluster gestito da Unified Manager. Il monitoraggio degli oggetti di archiviazione fornisce una panoramica delle prestazioni del cluster e degli oggetti e include il monitoraggio degli eventi relativi alle prestazioni. È possibile visualizzare le prestazioni e gli eventi a un livello elevato oppure è possibile analizzare più approfonditamente i dettagli delle prestazioni degli oggetti e degli eventi delle prestazioni.

Questo è un esempio delle tante possibili navigazioni degli oggetti cluster:

1. Dalla pagina Dashboard, esamina i dettagli nel pannello Capacità delle prestazioni per identificare il cluster che utilizza la maggiore capacità delle prestazioni e fai clic sul grafico a barre per passare all'elenco dei nodi per quel cluster.
2. Identifica il nodo con il valore di capacità di prestazioni più elevato utilizzato e fai clic su quel nodo.
3. Dalla pagina Nodo/Esplora prestazioni, fare clic su **Aggregati su questo nodo** dal menu Visualizza e confronta.
4. Identifica l'aggregato che utilizza la maggiore capacità di prestazioni e fai clic su tale aggregato.
5. Dalla pagina Esplora aggregato/prestazioni, fare clic su **Volumi su questo aggregato** dal menu Visualizza e confronta.

6. Identificare i volumi che utilizzano il maggior numero di IOPS.

È opportuno esaminare questi volumi per verificare se applicare una policy QoS o una policy Performance Service Level, oppure modificare le impostazioni della policy, in modo che tali volumi non utilizzino una percentuale così elevata di IOPS sul cluster.

Dashboard All Clusters

Management Actions

- Enable takeover on panic (2)
- Disable telnet (2)
- Enable volume autogrow (9)

Capacity

31 events (No new in past 24 hours)

CLUSTER	USED	DAYS TO FULL	REDUCTION
opm-sl...icity	40.5 TB	< 1 month	13.0:1
umeng...1-02	83.6 TB	51 days	8.0:1
sysmgr...0-1-8	33 TB	149 days	8.3:1

Performance Capacity

No new events

CLUSTER	USED	DAYS TO FULL
umeng-aff220-01-02	83%	< 1 month
sysmgr-fas8060-1-8	49%	< 1 month
fas8040-206-21	46%	77 days

Nodes Last updated: Nov 15, 2019, 10:48 AM

VIEW Nodes on umeng-aff220-01-02 Search Nodes Filter Hardware Inventory Report

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Show / Hide

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,333 IOPS	221 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	42%	6.1

Node / Performance : umeng-aff220-01

Summary Explorer Failover Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node Filter

Aggregate	Latency	IOPS	MB/s	Perf...
NSLM12_002	12.4 ...	47.51...	5.8 M...	8 %
NSLM12_001	11.4 ...	216 L...	4.33 ...	5 %

Aggregate / Performance : NSLM12_002

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate Filter

Volume	Latency	IOPS	MB/s
suchita_vmaware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchita_vmaware_d...	3.82 ms...	4,775 L...	18.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

Monitoraggio delle prestazioni del cluster e navigazione

È possibile monitorare le prestazioni di tutti i cluster gestiti da Unified Manager. Il monitoraggio dei cluster fornisce una panoramica delle prestazioni dei cluster e degli oggetti e include il monitoraggio degli eventi relativi alle prestazioni. È possibile

visualizzare le prestazioni e gli eventi a un livello elevato oppure è possibile analizzare più approfonditamente i dettagli delle prestazioni e degli eventi delle prestazioni del cluster e dell'oggetto.

Questo è un esempio dei tanti possibili percorsi di navigazione delle prestazioni del cluster:

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Per visualizzare informazioni sulle prestazioni in tali aggregati, selezionare la vista Prestazioni: Tutti gli aggregati.
3. Identifica l'aggregato che vuoi analizzare e fai clic sul nome dell'aggregato per accedere alla pagina Esplora aggregati/prestazioni.
4. Facoltativamente, seleziona altri oggetti da confrontare con questo aggregato nel menu Visualizza e confronta, quindi aggiungi uno degli oggetti al riquadro di confronto.

Le statistiche per entrambi gli oggetti appariranno nei grafici dei contatori per consentirne il confronto.

5. Nel riquadro Confronto a destra nella pagina Explorer, fare clic su **Zoom vista** in uno dei grafici dei contatori per visualizzare i dettagli sulla cronologia delle prestazioni 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%	< 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	Latency	IOPS	MB/s	Perf...
aggr3	5.06 ...	3.06 ...	< 1 M...	6%
aggr_evt	0.29 ...	3.79 ...	< 1 M...	< 1%
aggr_automation	0.27...	6.35 ...	< 1 M...	< 1%

Comparing
1 Additional Object
aggr4
aggr3

Events for Aggregate: aggr4
No data to display

Latency
Latency - Total view (ms/op)
aggr4
aggr3
Nov 14, 2019, 6:39 AM
12:00 AM Nov 15, 2019, 12:00 AM
Zoom View

Latency for Aggregate: aggr4

Last updated: Nov 15, 2019, 1:23 PM

Event Timeline: aggr4
Critical Events
Error Events
Warning Events
Information Events
No data to display

Comparing Objects
aggr4
aggr3
Latency - Total view (ms/op)
aggr4
aggr3
Nov 14, 2019, 1:24 AM
Nov 15, 2019, 12:00 AM Nov 15, 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 dell'indagine sugli eventi

Le pagine dei dettagli degli eventi di Unified Manager forniscono una panoramica approfondita di qualsiasi evento di performance. Ciò è utile quando si analizzano eventi relativi alle prestazioni, durante la risoluzione dei problemi e durante la messa a punto delle prestazioni del sistema.

A seconda del tipo di evento di performance, potresti visualizzare uno dei due tipi di pagine di dettaglio dell'evento:

- Pagina dei dettagli dell'evento per gli eventi dei criteri di soglia definiti dall'utente e dal sistema
- Pagina dei dettagli dell'evento per gli eventi della politica di soglia dinamica

Questo è un esempio di navigazione di indagine sugli eventi.

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.
2. Dal menu Visualizza, fare clic su **Eventi prestazioni attivi**.
3. Fare clic sul nome dell'evento che si desidera analizzare per visualizzare la pagina Dettagli evento.
4. Visualizza la descrizione dell'evento e rivedi le azioni suggerite (ove disponibili) per visualizzare maggiori dettagli sull'evento che potrebbero aiutarti a risolvere il problema. È possibile fare clic sul pulsante **Analizza carico di lavoro** per visualizzare grafici dettagliati delle prestazioni che consentono di analizzare ulteriormente il problema.

Event Management

Last updated: Nov 15, 2019, 11:23 AM

VIEW

Active performance events

Search Events

Filter

Assign To

Acknowledge

Mark as Resolved

Add Alert

Show / Hide

Triggered Time	Severity	State	Impact Lev	Impact Area	Name	Source	Source Ty
Nov 14, 2019, 11:39 AM		New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs2:/julia_feb12_vol3	Volume
Nov 14, 2019, 11:39 AM		New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_non_shared_3	Volume
Nov 15, 2019, 5:04 AM		New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	suchita_vmwvar...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM		New	Risk	Performance	Workload LUN Latency ...Service Level Policy	iscsi_boot/ia.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM		New	Risk	Performance	Workload LUN Latency ...Service Level Policy	iscsi_boot/ia.../ocum-c220-07	LUN

Event: QoS Volume Peak IOPS/TB Warning Threshold Breached

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM_vs7_Performance_2_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.

Actions

Suggested Actions to Fix The Issue

Troubleshoot

Analyze Workload

Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput,

- Leave the QoS configuration setting as it is.

Event Information

EVENT TRIGGER TIME	SEVERITY	SOURCE
Nov 14, 2019, 11:39 AM	Warning	vs7:/julia_non_shared_3
STATE	IMPACT LEVEL	SOURCE TYPE
New	Risk	Volume
EVENT DURATION	IMPACT AREA	ION CLUSTER
1 day 40 minutes	Performance	ocum-mobility-01-02
LAST SEEN		AFFECTED OBJECTS COUNT
Nov 15, 2019, 11:19 AM		1
		TRIGGERED POLICY
		QoS Peak IOPS/TB threshold

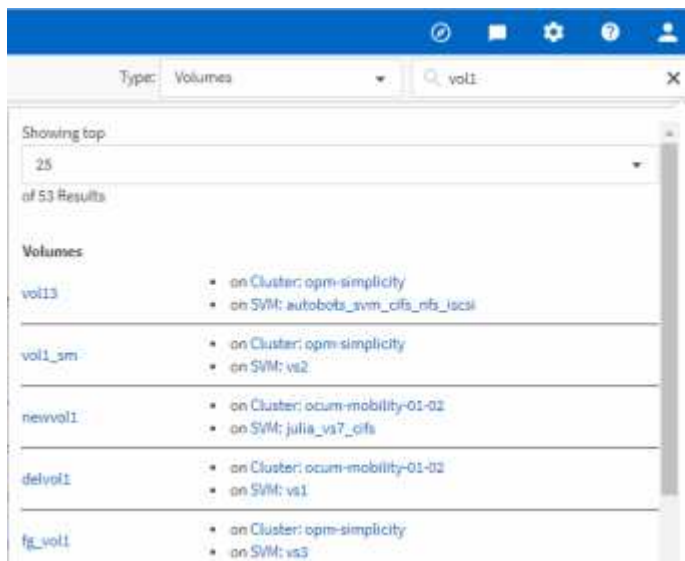
Cerca oggetti di archiviazione

Per accedere rapidamente a un oggetto specifico, puoi utilizzare il campo **Cerca tutti gli oggetti di archiviazione** nella parte superiore della barra dei menu. Questo metodo di ricerca globale su 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 archiviazione e possono essere filtrati utilizzando il menu a discesa. Una ricerca valida deve contenere almeno tre caratteri.

La ricerca globale visualizza il numero totale di risultati, ma sono accessibili solo i primi 25 risultati della ricerca. Per questo motivo, la funzionalità di ricerca globale può essere considerata uno strumento di scelta rapida per trovare elementi specifici se si conoscono gli elementi che si desidera individuare rapidamente. Per ottenere risultati di ricerca completi, è possibile utilizzare la ricerca nelle pagine dell'inventario degli oggetti e la relativa funzionalità di filtraggio.

È possibile fare clic sulla casella a discesa e selezionare **Tutti** per effettuare una ricerca simultanea in tutti gli oggetti e gli eventi. In alternativa, è possibile fare clic sulla casella a discesa per specificare il tipo di oggetto. Digitare almeno tre caratteri del nome dell'oggetto o dell'evento nel campo **Cerca tutti gli oggetti di archiviazione**, quindi premere **Invio** per visualizzare i risultati della ricerca, ad esempio:

- Cluster: nomi dei cluster
- Nodi: nomi dei nodi
- Aggregati: nomi aggregati
- SVM: nomi SVM
- Volumi: nomi dei volumi
- LUN: percorsi LUN



I 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 **Cerca tutti gli oggetti di archiviazione** viene visualizzato un elenco di tutti i volumi i cui nomi contengono questi caratteri. Per le ricerche di oggetti, puoi fare clic su qualsiasi risultato di ricerca per passare alla pagina Performance Explorer di quell'oggetto. Per le ricerche di eventi, cliccando su un elemento nel risultato della ricerca si accede alla pagina Dettagli evento.

Filtra il contenuto della pagina dell'inventario

È possibile filtrare i dati della pagina dell'inventario in Unified Manager per individuare rapidamente i dati in base a criteri specifici. È possibile utilizzare i filtri per restringere il contenuto delle pagine di Unified Manager in modo da visualizzare solo i risultati di proprio interesse. Questo fornisce un metodo molto efficiente per visualizzare solo i dati che ti interessano.

Utilizza **Filtro** per personalizzare la visualizzazione della griglia in base alle tue preferenze. Le opzioni di filtro disponibili si basano sul tipo di oggetto visualizzato nella griglia. Se sono attualmente applicati dei filtri, il numero di filtri applicati viene visualizzato a destra del pulsante Filtro.

Sono supportati tre tipi di parametri di filtro.

Parametro	Validazione
Stringa (testo)	Gli operatori sono contiene , inizia con , termina con e non contiene .
Numero	Gli operatori sono maggiore di , minore di , nell'ultimo e tra .
Enum (testo)	Gli operatori sono is e is not .

I campi Colonna, Operatore e Valore sono obbligatori per ciascun filtro; i filtri disponibili riflettono le colonne filtrabili nella pagina corrente. Il numero massimo di filtri che puoi 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 Filtraggio.

1. Nella parte superiore della pagina, fare clic sul pulsante **Filtro**. Viene visualizzato il pannello 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, seleziona o immetti un valore per completare il filtro per quell'oggetto.
5. Per aggiungere un altro filtro, fare clic su **+Aggiungi filtro**. Viene visualizzato un campo filtro aggiuntivo. Completare questo filtro utilizzando la procedura descritta nei passaggi precedenti. Tieni presente che dopo aver aggiunto il quarto filtro, il pulsante **+Aggiungi filtro** non verrà 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 Filtro.
7. Utilizzare il pannello Filtraggio per rimuovere singoli filtri facendo clic sull'icona del cestino a destra del filtro da rimuovere.
8. Per rimuovere tutti i filtri, fare clic su **Reimposta** nella parte inferiore del pannello di filtraggio.

Esempio di filtraggio

L'illustrazione mostra il pannello Filtraggio con tre filtri. Il pulsante **+Aggiungi filtro** viene visualizzato quando si hanno meno del massimo di quattro filtri.

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
+ Add Filter				
				Cancel Apply Filter

Dopo aver cliccato su **Applica filtro**, il pannello Filtraggio si chiude, applica i filtri e mostra il numero di filtri applicati (3).

Monitorare le prestazioni del cluster dalla Dashboard

La dashboard di Unified Manager fornisce alcuni pannelli che mostrano lo stato delle prestazioni di alto livello di tutti i cluster monitorati da questa istanza di Unified Manager. Consente di valutare le prestazioni complessive dei cluster gestiti e di annotare, individuare o assegnare rapidamente per la risoluzione eventuali eventi specifici identificati.

Comprendere i pannelli delle prestazioni nella Dashboard

La dashboard di Unified Manager fornisce alcuni pannelli che mostrano lo stato delle prestazioni di alto livello per tutti i cluster monitorati nel tuo ambiente. È possibile scegliere di visualizzare lo stato di tutti i cluster o di un singolo cluster.

Oltre a mostrare informazioni sulle prestazioni, la maggior parte dei pannelli mostra anche il numero di eventi attivi in quella categoria e il numero di nuovi eventi aggiunti nelle 24 ore precedenti. Queste informazioni ti aiutano a decidere quali cluster potresti dover 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 di Gestione eventi filtrata per visualizzare gli eventi in quella categoria.

I pannelli seguenti forniscono informazioni sullo stato delle prestazioni.

- **Pannello Capacità di prestazione**

Quando si visualizzano tutti i cluster, questo pannello mostra il valore della capacità di prestazione per ciascun cluster (calcolato sulla media dell'ora precedente) e il numero di giorni necessari affinché la capacità di prestazione raggiunga il limite superiore (in base al tasso di crescita giornaliero). Facendo clic sul grafico a barre si accede alla pagina dell'inventario dei nodi per quel cluster. Si noti che la pagina Inventario nodi visualizza la capacità prestazionale media delle 72 ore precedenti, pertanto questo valore potrebbe non corrispondere al valore della Dashboard.

Quando si visualizza un singolo cluster, questo pannello mostra la capacità delle prestazioni del cluster, gli IOPS totali e i valori di throughput totale.

- **Pannello IOPS del carico di lavoro**

Quando è abilitata la gestione attiva del carico di lavoro e quando si visualizza un singolo cluster, questo

pannello mostra il numero totale di carichi di lavoro attualmente in esecuzione in un determinato intervallo di IOPS.

- **Pannello Prestazioni del carico di lavoro**

Quando la gestione attiva del carico di lavoro è abilitata, questo pannello visualizza il numero totale di carichi di lavoro conformi e non conformi assegnati a ciascun livello di servizio delle prestazioni definito. Facendo clic su un grafico a barre si accede ai carichi di lavoro assegnati a tale criterio nella pagina Carichi di lavoro.

- **Pannello Panoramica sull'utilizzo**

Quando si visualizzano tutti i cluster, è possibile scegliere di visualizzarli ordinati in base al numero più elevato di IOPS o di throughput (MB/s).

Quando si visualizza un singolo cluster, è possibile scegliere di visualizzare i carichi di lavoro su quel cluster ordinati in base al numero più elevato di IOPS o di throughput (MB/s).

Messaggi e descrizioni dei banner sulle prestazioni

Unified Manager può visualizzare messaggi banner nella pagina Notifiche (dalla campana delle notifiche) per avvisarti di problemi di stato per un cluster specifico.

Messaggio banner	Descrizione	Risoluzione
No performance data is being collected from cluster <code>cluster_name</code> . Restart Unified Manager to correct this issue.	Il servizio di raccolta Unified Manager è stato arrestato e non vengono raccolti dati sulle prestazioni da alcun cluster.	Riavviare Unified Manager per correggere il problema. Se il problema persiste, contattare l'assistenza tecnica.
More than x hour(s) of historical data is being collected from cluster <code>cluster_name</code> . Current data collections will start after all historical data is collected.	È attualmente in esecuzione un ciclo di raccolta della continuità dei dati per recuperare i dati sulle prestazioni al di fuori del ciclo di raccolta delle prestazioni del cluster in tempo reale.	Non è richiesta alcuna azione. I dati sulle prestazioni attuali saranno raccolti una volta completato il 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 riuscito a raccogliere i dati sulle prestazioni correnti per qualche motivo.

Modificare l'intervallo di raccolta delle statistiche sulle prestazioni

L'intervallo di raccolta predefinito per le statistiche sulle prestazioni è di 5 minuti. È possibile modificare questo intervallo a 10 o 15 minuti se si nota che le raccolte provenienti da cluster di grandi dimensioni non vengono completate entro il tempo predefinito. Questa impostazione influisce sulla raccolta di statistiche da tutti i cluster

monitorati da questa istanza di Unified Manager.

Prima di iniziare

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 sulle prestazioni che non terminano in tempo è indicato dai messaggi del banner `Unable to consistently collect from cluster <cluster_name> O Data collection is taking too long on cluster <cluster_name>.`

Dovresti modificare l'intervallo di raccolta solo quando necessario a causa di un problema di raccolta delle statistiche. Non modificare questa impostazione per nessun altro motivo.



La modifica di questo valore rispetto all'impostazione predefinita di 5 minuti può influire sul numero e sulla frequenza degli eventi di prestazione segnalati da Unified Manager. Ad esempio, le soglie di prestazioni definite dal sistema attivano eventi quando la policy viene superata per 30 minuti. Quando si utilizzano raccolte di 5 minuti, la norma deve essere superata per sei raccolte consecutive. Per le raccolte di 15 minuti, la norma deve essere superata solo per due periodi di raccolta.

Un messaggio nella parte inferiore della pagina Configurazione cluster indica l'intervallo corrente di raccolta dei dati statistici.

Passi

1. Accedere tramite SSH come utente di manutenzione all'host Unified Manager.

Vengono visualizzati i prompt della console di manutenzione di Unified Manager.

2. Digitare il numero dell'opzione di menu denominata **Configurazione intervallo di polling delle prestazioni**, quindi premere Invio.
3. Se richiesto, immettere nuovamente la password dell'utente addetto alla manutenzione.
4. Digitare il numero per il nuovo intervallo di polling che si desidera impostare, quindi premere Invio.

Se hai modificato l'intervallo di raccolta di Unified Manager in 10 o 15 minuti e hai una connessione corrente a un provider di dati esterno (ad esempio Graphite), devi modificare l'intervallo di trasmissione del provider di dati in modo che sia uguale o maggiore dell'intervallo di raccolta di Unified Manager.

Risolvi i problemi dei carichi di lavoro utilizzando l'analizzatore dei carichi di lavoro

L'analizzatore del carico di lavoro consente di visualizzare in un'unica pagina importanti criteri di integrità e prestazioni per un singolo carico di lavoro, per agevolare la risoluzione dei problemi. Visualizzando tutti gli eventi attuali e passati per un carico di lavoro, è possibile farsi un'idea più precisa del motivo per cui il carico di lavoro potrebbe presentare un problema di prestazioni o capacità.

Utilizzando questo strumento è anche possibile determinare se la causa dei problemi di prestazioni di un'applicazione è l'archiviazione o se il problema è dovuto a un problema di rete o ad altri problemi correlati.

È possibile avviare questa funzionalità da diversi punti dell'interfaccia utente:

- Dalla selezione Analisi del carico di lavoro nel menu di navigazione a sinistra
- Dalla pagina dei dettagli dell'evento cliccando sul pulsante **Analizza carico di lavoro**
- Da qualsiasi pagina dell'inventario del carico di lavoro (volume, LUN, carico di lavoro, condivisione NFS o condivisione SMB/CIFS), facendo clic sull'icona Altro , quindi **Analizza carico di lavoro**
- Dalla pagina Macchine virtuali facendo clic sul pulsante **Analizza carico di lavoro** da qualsiasi oggetto Datastore

Quando avvii lo strumento dal menu di navigazione a sinistra, puoi immettere il nome di qualsiasi carico di lavoro che desideri analizzare e selezionare l'intervallo di tempo per il quale desideri risolvere i problemi. Quando si avvia lo strumento da una qualsiasi delle pagine di inventario del carico di lavoro o della macchina virtuale, il nome del carico di lavoro viene compilato automaticamente e i dati del carico di lavoro vengono presentati 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 visualizza l'analizzatore del carico di lavoro?

La pagina dell'analizzatore del carico di lavoro visualizza informazioni su eventuali eventi correnti che potrebbero influire sul carico di lavoro, suggerimenti per risolvere potenzialmente il problema che causa l'evento e grafici per analizzare la cronologia delle prestazioni e della capacità.

Nella parte superiore della pagina è possibile specificare il nome del carico di lavoro (volume o LUN) che si desidera analizzare e l'intervallo di tempo per il quale 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 mostrano i risultati dell'analisi e i grafici delle prestazioni e della capacità.



I grafici del carico di lavoro per le LUN non forniscono lo stesso livello di statistiche dei grafici per i volumi, pertanto si noteranno delle differenze quando si analizzano questi due tipi di carichi di lavoro.

• Area riassuntiva eventi

Visualizza una breve panoramica del numero e dei tipi di eventi verificatisi nel periodo di tempo considerato. Quando sono presenti eventi di diverse aree di impatto (ad esempio, prestazioni 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 l'intervallo di tempo specificato, per alcuni eventi viene fornito un elenco di suggerimenti per risolvere il problema.

• Cronologia dell'evento

Mostra tutte le occorrenze degli eventi durante l'intervallo di tempo specificato. Passa il cursore su ogni evento per visualizzarne il nome.

Se sei arrivato a questa pagina cliccando sul pulsante **Analizza carico di lavoro** dalla pagina dei dettagli dell'evento, l'icona dell'evento selezionato apparirà più grande, così potrai identificarlo.

• Area grafici delle prestazioni

Visualizza grafici per latenza, throughput (sia IOPS che MB/s) e utilizzo (sia per il nodo che per l'aggregato) in base all'intervallo di tempo selezionato. È possibile fare clic sul collegamento Visualizza dettagli sulle prestazioni per visualizzare la pagina Esplora prestazioni per il carico di lavoro nel caso in cui si desideri eseguire ulteriori analisi.

- **Latenza** mostra la latenza del carico di lavoro nell'intervallo di tempo selezionato. Il grafico ha tre visualizzazioni che consentono di vedere:
 - Latenza **totale**
 - **Ripartizione** della latenza (suddivisa per letture, scritture e altri processi)
 - Latenza dei **componenti del cluster** (suddivisa per componente del cluster)

Vedere "[Componenti del cluster e perché possono essere in competizione](#)" per una descrizione dei componenti del cluster visualizzati qui. **Throughput** mostra sia gli IOPS che il throughput MB/s per il carico di lavoro nell'intervallo di tempo selezionato. Il grafico presenta quattro visualizzazioni che consentono di visualizzare: * Throughput totale * Throughput ripartito (suddiviso per letture, scritture e altri processi) * Throughput cloud (MB/s utilizzati per scrivere e leggere dati dal cloud; per i carichi di lavoro che suddividono la capacità in livelli nel cloud) * IOPS con previsione (una previsione dei valori di throughput IOPS massimo e minimo previsti nell'intervallo di tempo) Questo grafico visualizza anche le impostazioni della soglia di throughput massima e minima della qualità del servizio (QoS), se configurate, in modo da poter vedere dove il sistema potrebbe limitare intenzionalmente il throughput con i criteri QoS. **Utilizzo** mostra l'utilizzo sia dell'aggregato che del nodo su cui è in esecuzione il carico di lavoro nell'intervallo di tempo selezionato. Da qui puoi vedere se il tuo aggregato o nodo sono sovrautilizzati, causando probabilmente un'elevata latenza. Quando si analizzano i volumi FlexGroup, nei grafici di utilizzo sono elencati più nodi e più aggregati.

• Area del grafico della capacità

Visualizza grafici sulla capacità dei dati e sulla capacità degli snapshot per l'ultimo mese per il carico di lavoro.

Per i volumi, è possibile fare clic sul collegamento Visualizza dettagli capacità per visualizzare la pagina Dettagli integrità per il carico di lavoro nel caso in cui si desideri eseguire ulteriori analisi. I LUN non forniscono questo collegamento perché non esiste una pagina con i dettagli sullo stato di salute per i LUN.

- **Capacity View** mostra lo spazio totale disponibile allocato per il carico di lavoro e lo spazio logico utilizzato (dopo tutte le ottimizzazioni NetApp).
- **Snapshot View** mostra lo spazio totale riservato alle copie Snapshot e la quantità di spazio attualmente utilizzata. Si noti che le LUN non forniscono una vista snapshot.
- **Cloud Tier View** mostra quanta capacità viene utilizzata nel livello di prestazioni locale e quanta viene utilizzata nel livello cloud. Questi grafici includono una stima del tempo rimanente prima che la capacità per questo carico di lavoro sia piena. Queste informazioni si basano sull'utilizzo storico e richiedono almeno 10 giorni di dati. Quando la capacità residua è inferiore a 30 giorni, Unified Manager identifica lo storage come "quasi pieno".

Quando dovrei usare l'analizzatore del carico di lavoro?

In genere, l'analizzatore del carico di lavoro viene utilizzato per risolvere un problema di latenza segnalato da un utente, per analizzare più approfonditamente un evento o un avviso segnalato o per esplorare un carico di lavoro che si nota funzionare in modo anomalo.

Nel caso in cui gli utenti ti abbiano contattato per dirti che l'applicazione che stanno utilizzando è molto lenta, puoi controllare i grafici di latenza, produttività e utilizzo per il carico di lavoro su cui è in esecuzione l'applicazione per verificare se l'archiviazione è la causa del problema di prestazioni. È possibile utilizzare anche il grafico della capacità per verificare se la capacità è bassa, poiché un sistema ONTAP in cui la capacità è utilizzata per oltre l'85% può causare problemi di prestazioni. Questi grafici ti aiuteranno a determinare se il problema è causato dall'archiviazione, da un problema di rete o da altri problemi correlati.

Nel caso in cui Unified Manager abbia generato un evento di prestazioni e si desideri esaminare più approfonditamente la causa del problema, è possibile avviare l'analizzatore del carico di lavoro dalla pagina Dettagli evento facendo clic sul pulsante **Analizza carico di lavoro** per ricercare alcuni trend di latenza, produttività e capacità per il carico di lavoro.

Nel caso in cui si noti un carico di lavoro che sembra funzionare in modo anomalo durante la visualizzazione di una qualsiasi pagina di inventario del carico di lavoro (volume, LUN, carico di lavoro, condivisione NFS o condivisione SMB/CIFS), è possibile fare clic sull'icona Altro , quindi **Analizza carico di lavoro** per aprire la pagina Analisi carico di lavoro ed esaminare ulteriormente il carico di lavoro.

Utilizzare l'analizzatore del carico di lavoro

Esistono molti modi per avviare l'analizzatore del carico di lavoro dall'interfaccia utente. Qui descriviamo come avviare lo strumento dal riquadro di navigazione a sinistra.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Analisi del carico di lavoro**.

Viene visualizzata la pagina Analisi del carico di lavoro.

2. Se conosci il nome del carico di lavoro, inseriscilo. Se non si è sicuri del nome completo, immettere almeno 3 caratteri e il sistema visualizzerà un elenco di carichi di lavoro che corrispondono alla stringa.
3. Seleziona l'intervallo di tempo se desideri visualizzare le statistiche per un periodo più lungo delle 2 ore predefinite e fai clic su **Applica**.
4. Visualizza l'area Riepilogo per vedere gli eventi che si sono verificati durante l'intervallo di tempo.
5. Visualizza i grafici delle prestazioni e della capacità per vedere quando una delle metriche è anomala e verificare se qualche evento è in linea con la voce anomala.

Monitora le prestazioni del cluster dalla pagina di destinazione del cluster delle prestazioni

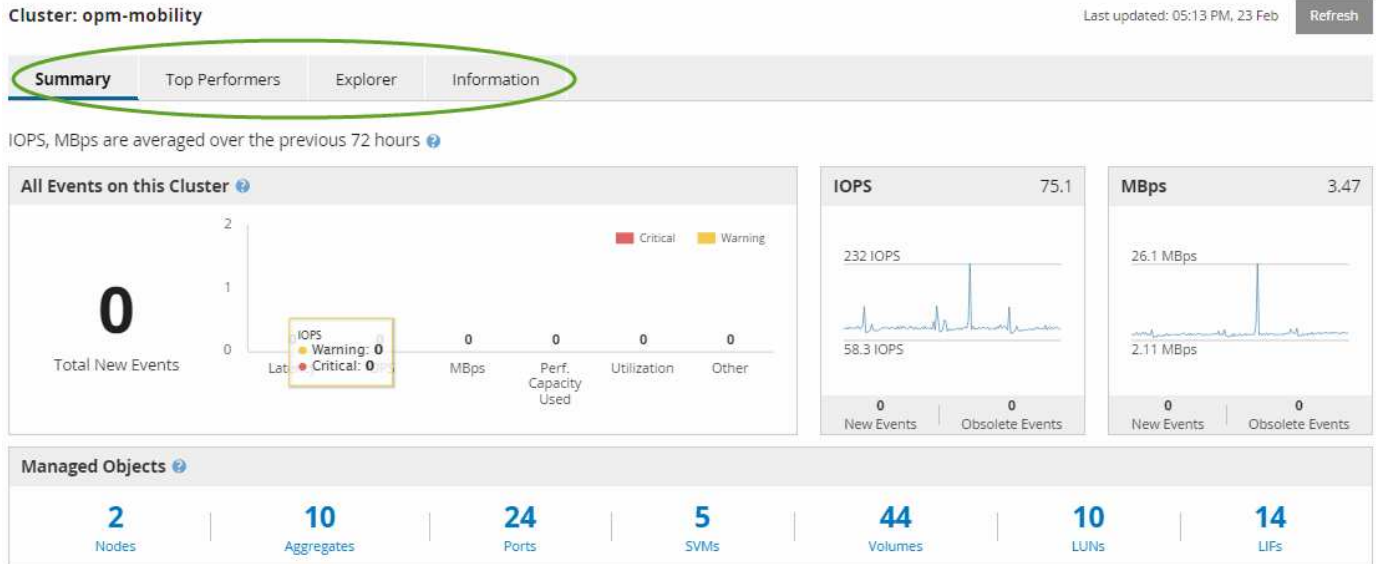
La pagina di destinazione del cluster delle prestazioni visualizza lo stato delle prestazioni di alto livello di un cluster selezionato monitorato da un'istanza di Unified Manager. Questa pagina consente di valutare le prestazioni complessive di un cluster specifico e di annotare, individuare o assegnare rapidamente per la risoluzione tutti gli eventi specifici del cluster identificati.

Comprendere la pagina di destinazione del Performance Cluster

La pagina di destinazione del cluster delle prestazioni fornisce una panoramica di alto livello delle prestazioni di un cluster selezionato, con particolare attenzione allo stato delle prestazioni dei primi 10 oggetti all'interno del cluster. I problemi di prestazioni

vengono visualizzati nella parte superiore della pagina, nel pannello Tutti gli eventi in questo cluster.

La pagina di destinazione del Performance Cluster fornisce una panoramica di alto livello di ciascun cluster gestito da un'istanza di Unified Manager. Questa pagina fornisce informazioni su eventi e prestazioni e consente di monitorare e risolvere i problemi dei cluster. L'immagine seguente mostra un esempio della landing page del Performance Cluster per il cluster denominato opm-mobility:



Il conteggio degli eventi nella pagina Riepilogo cluster potrebbe non corrispondere al conteggio degli eventi nella pagina Inventario eventi prestazioni. Ciò avviene perché la pagina Riepilogo cluster può mostrare un evento in ciascuna barra Latenza e Utilizzo quando vengono violate le policy di soglia combinate, mentre la pagina Inventario eventi prestazioni mostra un solo evento quando viene violata una policy combinata.



Se un cluster è stato rimosso dalla gestione di Unified Manager, lo stato **Rimosso** viene visualizzato a destra del nome del cluster nella parte superiore della pagina.

Pagina di destinazione del Performance Cluster

La pagina di destinazione del cluster di prestazioni visualizza lo stato delle prestazioni di alto livello di un cluster selezionato. La pagina consente di accedere ai dettagli completi di ciascun contatore delle prestazioni per gli oggetti di archiviazione nel cluster selezionato.

La pagina di destinazione del cluster di prestazioni include quattro schede che suddividono i dettagli del cluster in quattro aree di informazioni:

- Pagina di riepilogo
 - Riquadro Eventi cluster
 - Grafici delle prestazioni MB/s e IOPS
 - Riquadro Oggetti gestiti
- Pagina dei migliori artisti
- Pagina Explorer

- Pagina informativa

Pagina di riepilogo del cluster di prestazioni

La pagina Riepilogo cluster prestazioni fornisce un riepilogo degli eventi attivi, delle prestazioni IOPS e delle prestazioni MB/s per un cluster. Questa pagina include anche il conteggio totale degli oggetti di archiviazione nel cluster.

Riquadro eventi prestazioni cluster

Il riquadro Eventi prestazioni cluster visualizza le statistiche sulle prestazioni e tutti gli eventi attivi per il cluster. Questa funzionalità è particolarmente utile quando si monitorano i cluster e tutte le prestazioni e gli eventi correlati.

Riquadro Tutti gli eventi in questo cluster

Il riquadro Tutti gli eventi su questo cluster visualizza tutti gli eventi di prestazioni del cluster attivi nelle 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 archiviazione in questo cluster. È possibile fare clic sul collegamento Eventi attivi totali per passare alla pagina Inventario eventi, che è filtrata per visualizzare questi eventi.

Il grafico a barre Eventi attivi totali per il cluster mostra il numero totale di eventi critici e di avviso attivi:

- Latenza (totale per nodi, aggregati, SVM, volumi, LUN e namespace)
- IOPS (totale per cluster, nodi, aggregati, SVM, volumi, LUN e namespace)
- MB/s (totale per cluster, nodi, aggregati, SVM, volumi, LUN, namespace, porte e LIF)
- Capacità di prestazione utilizzata (totale per nodi e aggregati)
- Utilizzo (totale per nodi, aggregati e porte)
- Altro (rapporto di cache miss per volumi)

L'elenco contiene eventi di prestazioni attivi attivati da criteri di soglia definiti dall'utente, criteri di soglia definiti dal sistema e soglie dinamiche.

I dati del grafico (barre del contatore verticale) vengono visualizzati in rosso (■) per eventi critici e giallo (■) per gli eventi di avviso. Posiziona il cursore su ogni barra del contatore verticale per visualizzare il tipo e il numero effettivi di eventi. È possibile fare clic su **Aggiorna** per aggiornare i dati del pannello del contatore.

È possibile mostrare o nascondere gli eventi critici e di avviso nel grafico delle prestazioni 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 da banco

I pannelli dei contatori mostrano l'attività del cluster e gli eventi di prestazione delle 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 contatore fornisce una panoramica di alto livello dello stato di IOPS del cluster per il periodo di 72

ore precedente. È possibile posizionare il cursore sulla linea di tendenza del grafico per visualizzare il valore IOPS per un periodo di 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 contatore fornisce una panoramica di alto livello dello stato di salute del cluster in MB/s per il periodo di 72 ore precedenti. È possibile posizionare il cursore sulla linea di tendenza del grafico per visualizzare il valore MB/s per un periodo di tempo specifico.

Il numero in alto a destra del grafico, nella barra grigia, è il valore medio delle ultime 72 ore. I numeri mostrati nella parte inferiore e superiore del grafico della linea di tendenza rappresentano i valori minimo e massimo dell'ultimo periodo di 72 ore. La barra grigia sotto il grafico contiene il conteggio degli eventi attivi (nuovi e riconosciuti) e degli eventi obsoleti dell'ultimo periodo di 72 ore.

I pannelli del contatore contengono due tipi di eventi:

- **Attivo**

Indica che l'evento di performance è attualmente attivo (nuovo o riconosciuto). Il problema che ha causato l'evento non è stato risolto o non è stato risolto. Il contatore delle prestazioni per l'oggetto di archiviazione rimane al di sopra della soglia delle prestazioni.

- **Obsoleto**

Indica che l'evento non è più attivo. Il problema che ha causato l'evento è stato corretto o risolto. Il contatore delle prestazioni per l'oggetto di archiviazione non è più al di sopra della soglia delle prestazioni.

Per gli **Eventi attivi**, se è presente un evento, puoi posizionare il cursore sull'icona dell'evento e fare clic sul numero dell'evento per collegarti alla pagina Dettagli evento appropriata. Se è presente più di un evento, è possibile fare clic su **Visualizza tutti gli eventi** per visualizzare la pagina Inventario eventi, che viene filtrata per mostrare tutti gli eventi per il tipo di contatore di oggetti selezionato.

Riquadro Oggetti gestiti

Il riquadro Oggetti gestiti nella scheda Riepilogo prestazioni fornisce una panoramica di alto livello dei tipi di oggetti di archiviazione e dei conteggi per il cluster. Questo riquadro consente di monitorare lo stato degli oggetti in ciascun cluster.

Il conteggio degli oggetti gestiti è costituito da dati puntuali a partire dall'ultimo periodo di raccolta. Nuovi oggetti vengono scoperti a intervalli di 15 minuti.

Facendo clic sul numero collegato per qualsiasi tipo di oggetto viene visualizzata la pagina dell'inventario delle prestazioni dell'oggetto per quel tipo di oggetto. La pagina dell'inventario degli oggetti è filtrata per mostrare solo gli oggetti presenti in 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 un'unica unità per la protezione e il provisioning.

- **Porte**

Punto di connessione fisica sui nodi utilizzato per connettersi ad altri dispositivi su una rete.

- **VM di archiviazione**

Una macchina virtuale che fornisce accesso alla rete tramite indirizzi di rete univoci. Una SVM può fornire dati da uno spazio dei nomi distinto ed è amministrabile separatamente dal resto del cluster.

- **Volumi**

Un'entità logica che contiene dati utente accessibili tramite uno o più protocolli di accesso supportati. Il conteggio include sia i volumi FlexVol sia i volumi FlexGroup ; non include i componenti FlexGroup .

- **LUN**

Identificatore di un'unità logica Fibre Channel (FC) o di un'unità logica iSCSI. Un'unità logica corrisponde in genere a un volume di archiviazione ed è rappresentata all'interno del sistema operativo di un computer come un dispositivo.

- **Interfacce di rete**

Un'interfaccia di rete logica che rappresenta un punto di accesso alla rete per un nodo. Il conteggio include tutti i tipi di interfaccia.

Pagina dei migliori artisti

La pagina Migliori prestazioni visualizza gli oggetti di archiviazione con le prestazioni più elevate o più basse, in base al contatore delle prestazioni selezionato. Ad esempio, nella categoria VM di archiviazione, è possibile visualizzare le SVM con gli IOPS più elevati, la latenza più elevata o i MB/s più bassi. Questa pagina mostra anche se uno dei migliori performer ha eventi di performance attivi (nuovi o riconosciuti).

La pagina Top Performers visualizza al massimo 10 esemplari di ciascun oggetto. Si noti che l'oggetto Volume include sia i volumi FlexVol sia i volumi FlexGroup .

- **Intervallo di tempo**

È possibile selezionare un intervallo di tempo per visualizzare i risultati migliori; l'intervallo di tempo selezionato si applica a tutti gli oggetti di archiviazione. Intervalli di tempo disponibili:

- Ultima ora
- Ultime 24 ore
- Ultime 72 ore (predefinito)
- Ultimi 7 giorni

- **Metrico**

Fare clic sul menu **Metrica** per selezionare un contatore diverso. Le opzioni del contatore sono esclusive del tipo di oggetto. Ad esempio, i contatori disponibili per l'oggetto **Volumi** sono **Latenza**, **IOPS** e **MB/s**.

Modificando il contatore, i dati del pannello vengono ricaricati con i migliori risultati in base al contatore selezionato.

Contatori disponibili:

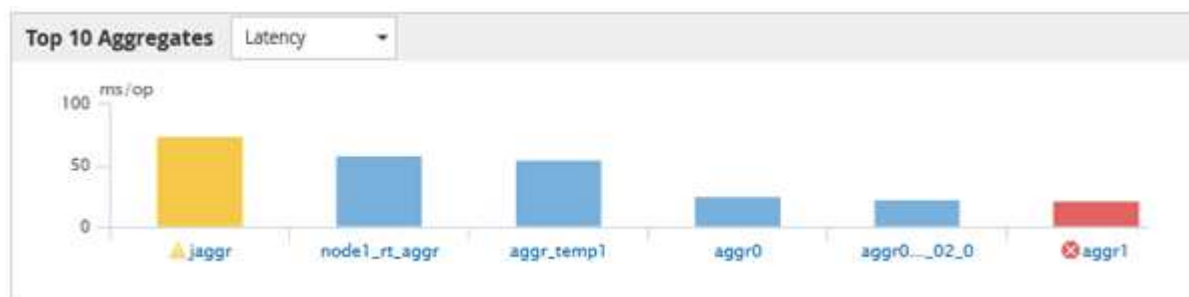
- Latenza
- IOPS
- MB/s
- Capacità di prestazione utilizzata (per nodi e aggregati)
- Utilizzo (per nodi e aggregati)

• Ordinare

Fare clic sul menu **Ordina** per selezionare un ordinamento crescente o decrescente per l'oggetto e il contatore selezionati. Le opzioni sono **Dal più alto al più basso** e **Dal più basso al più alto**. Queste opzioni consentono di visualizzare gli oggetti con le prestazioni più elevate o più basse.

• Bancone del bar

La barra del contatore nel grafico mostra le statistiche delle prestazioni per ciascun oggetto, rappresentate come una barra per quell'elemento. I grafici a barre sono codificati a colori. Se il contatore non supera una soglia di prestazione, la barra del contatore viene visualizzata in blu. Se è attiva una violazione della soglia (un evento nuovo o riconosciuto), la barra viene visualizzata nel colore dell'evento: gli eventi di avviso vengono visualizzati in giallo (■), e gli eventi critici vengono visualizzati in rosso (■). Le violazioni delle soglie sono ulteriormente segnalate da icone indicatrici di gravità degli eventi per gli avvisi e gli eventi critici.



Per ogni grafico, l'asse X mostra i migliori risultati per il tipo di oggetto selezionato. L'asse Y visualizza le unità applicabili al contatore selezionato. Facendo clic sul collegamento del nome dell'oggetto sotto ogni elemento del grafico a barre verticali si accede alla pagina di destinazione delle prestazioni per l'oggetto selezionato.

• Indicatore di gravità dell'evento

L'icona dell'indicatore **Evento di gravità** viene visualizzata a sinistra del nome di un oggetto per un evento critico attivo (⊗) o avvertimento (⚠) eventi nei grafici dei migliori performer. Fare clic sull'icona dell'indicatore **Evento di gravità** per visualizzare:

- **Un evento**

Consente di accedere alla pagina dei dettagli dell'evento.

- **Due o più eventi**

Consente di accedere alla pagina Inventario eventi, che viene filtrata per visualizzare tutti gli eventi per l'oggetto selezionato.

- **Pulsante Esporta**

Crea un .csv file che contiene i dati che compaiono nella barra del contatore. Puoi scegliere di creare il file per il singolo cluster che stai visualizzando o per tutti i cluster nel data center.

Monitorare le prestazioni utilizzando le pagine Inventario delle prestazioni

Le pagine relative alle prestazioni dell'inventario degli oggetti mostrano informazioni sulle prestazioni, eventi sulle prestazioni e stato dell'oggetto per tutti gli oggetti all'interno di una categoria di tipo di oggetto. Ciò fornisce una panoramica immediata dello stato delle prestazioni di ciascun oggetto all'interno di un cluster, ad esempio per tutti i nodi o tutti i volumi.

Le pagine sulle prestazioni dell'inventario degli oggetti forniscono una panoramica di alto livello dello stato degli oggetti, consentendo di valutare le prestazioni complessive di tutti gli oggetti e di confrontare i dati sulle prestazioni degli oggetti. È possibile perfezionare il contenuto delle pagine dell'inventario degli oggetti tramite ricerca, ordinamento e filtraggio. Ciò è utile quando si monitorano e si gestiscono le prestazioni degli oggetti, perché consente di individuare rapidamente gli oggetti con problemi di prestazioni e di avviare il processo di risoluzione dei problemi.

Nodes - Performance / All Nodes ⓘ

Last updated: Jan 17, 2019, 7:54 AM ↻

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

View		All Nodes	Search Nodes								
Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report							
☐	Status	Node	Latency	IOPS	MBps	Flash Cache Reads	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster
☐		ocum-mobility-02	10.2 ms/op	18,884 IOPS	156 MBps	N/A	81%	35%	16.6 TB	23.2 TB	ocum-mobility-01-02
☒		opm-simplicity-01	2.01 ms/op	39,358 IOPS	153 MBps	< 1%	119%	88%	4.88 TB	18.3 TB	opm-simplicity
☐		ocum-mobility-01	0.018 ms/op	< 1 IOPS	18.2 MBps	N/A	23%	18%	8.69 TB	15.7 TB	ocum-mobility-01-02
☐		opm-simplicity-02	17 ms/op	14,627 IOPS	124 MBps	< 1%	29%	20%	212 GB	5.88 TB	opm-simplicity

Per impostazione predefinita, gli oggetti nelle pagine dell'inventario delle prestazioni vengono ordinati in base alla criticità delle prestazioni dell'oggetto. Gli oggetti con nuovi eventi critici sulle prestazioni vengono elencati per primi, mentre gli oggetti con eventi di avviso vengono elencati per secondi. Ciò fornisce un'indicazione visiva immediata dei problemi che devono essere affrontati. Tutti i dati sulle prestazioni si basano su una media di 72 ore.

È possibile passare facilmente dalla pagina delle prestazioni dell'inventario degli oggetti alla pagina dei dettagli degli oggetti facendo clic sul nome dell'oggetto nella colonna del nome dell'oggetto. Ad esempio, nella pagina dell'inventario Prestazioni/Tutti i nodi, fare clic su un oggetto nodo nella colonna **Nodi**. La pagina dei dettagli dell'oggetto fornisce informazioni approfondite e dettagli sull'oggetto selezionato, incluso il confronto affiancato degli eventi attivi.

Visualizza le pagine dell'inventario delle prestazioni per tutti gli oggetti di archiviazione

È possibile utilizzare le pagine Inventario prestazioni per visualizzare un riepilogo delle informazioni sulle prestazioni relative a ciascuno degli oggetti di archiviazione disponibili, ad esempio cluster, aggregati, volumi e così via. È possibile collegarsi alle pagine dei dettagli dell'oggetto Performance per visualizzare informazioni dettagliate su un oggetto specifico.

Per impostazione predefinita, gli oggetti nelle pagine di visualizzazione vengono ordinati in base alla criticità dell'evento. Gli oggetti con eventi critici vengono elencati per primi, mentre gli oggetti con eventi di avviso vengono elencati per secondi. Ciò fornisce un'indicazione visiva immediata dei problemi che devono essere affrontati.

È possibile esportare i dati da queste pagine in valori separati da virgole(.csv) file, file Microsoft Excel(.xlsx), O(.pdf) documento utilizzando il pulsante **Report** e quindi utilizzare i dati esportati per creare report. Inoltre, puoi personalizzare la pagina e quindi programmare la creazione e l'invio periodico di un report tramite e-mail utilizzando il pulsante **Report programmati**.

Tutti i campi di queste pagine possono essere utilizzati nelle visualizzazioni personalizzate e nei report. Alcuni campi sono collegati a pagine correlate, consentendo una visualizzazione più dettagliata.

Prestazioni: visualizzazione di tutti i cluster

La vista Prestazioni: tutti i cluster mostra una panoramica degli eventi relativi alle prestazioni, dei dati e delle informazioni di configurazione per ciascun cluster monitorato da un'istanza di Unified Manager. Questa pagina consente di monitorare le prestazioni dei cluster e di risolvere i problemi relativi alle prestazioni e agli eventi di soglia.

È possibile assegnare o cancellare criteri di soglia delle prestazioni a qualsiasi oggetto nelle pagine dell'inventario degli oggetti utilizzando i pulsanti **Assegna criterio di soglia delle prestazioni** e **Cancella criterio di soglia delle prestazioni**.

Di seguito sono riportati alcuni campi importanti nella vista Prestazioni: tutti i cluster.

- FQDN del cluster: nome di dominio completo (FQDN) del cluster.
- IOPS: operazioni di input/output al secondo sul cluster.
- MB/s: la velocità effettiva del cluster, misurata in MiB al secondo.
- Campi capacità: capacità libera e totale in GiB.
- Nome host o indirizzo IP: nome host o indirizzo IP (IPv4 o IPv6) del LIF di gestione del cluster.
- Versione del sistema operativo: la versione del software ONTAP installata sul cluster.



Se sui nodi del cluster sono installate diverse versioni del software ONTAP , viene elencato il numero di versione più basso. È possibile visualizzare la versione ONTAP installata su ciascun nodo dalla vista Prestazioni: Tutti i nodi.

- Criterio di soglia: il criterio o i criteri di soglia delle prestazioni definiti dall'utente attivi su questo oggetto di archiviazione. È possibile posizionare il cursore sui nomi delle policy contenenti puntini di sospensione (...) per visualizzare il nome completo della policy o l'elenco dei nomi delle policy assegnati. I pulsanti Assegna criterio soglia prestazioni e Cancella criterio soglia prestazioni rimangono disabilitati finché non si selezionano uno o più oggetti facendo clic sulle caselle di controllo situate all'estrema sinistra.

Prestazioni: visualizzazione di tutti i volumi

La vista Prestazioni: tutti i volumi mostra una panoramica degli eventi relativi alle prestazioni, dei dati dei contatori e delle informazioni di configurazione per ciascun FlexVol volume e FlexGroup monitorato da un'istanza di Unified Manager. Ciò consente di monitorare rapidamente le prestazioni dei volumi e di risolvere i problemi di prestazioni e gli eventi di soglia.

Se vuoi analizzare la latenza e la produttività di un oggetto specifico, fai clic sul pulsante Altre opzioni  quindi **Analizza carico di lavoro** e potrai visualizzare grafici di prestazioni e capacità nella pagina Analisi del carico di lavoro. È possibile visualizzare i dettagli su System Manager, a condizione di disporre di credenziali valide per System Manager.



Per i volumi di protezione dei dati (DP), vengono visualizzati solo i valori del contatore per il traffico generato dall'utente. I volumi radice non vengono visualizzati in questa pagina.

Di seguito sono riportati alcuni campi importanti nella vista Prestazioni: Tutti i volumi.

- Stile: FlexVol o FlexGroup.
- Latenza: per i volumi FlexVol , questo è il tempo di risposta medio del volume per tutte le richieste di I/O, espresso in millisecondi per operazione. Per i volumi FlexGroup , questa è la latenza media di tutti i volumi costituenti.
- IOPS/TB: 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 prestazioni che può essere fornita da una determinata quantità di capacità di archiviazione.
- IOPS: per i volumi FlexVol , questo è il numero di operazioni di input/output al secondo per il volume. Per i volumi FlexGroup , questa è la somma degli IOPS per tutti i volumi costituenti.
- MB/s: per i volumi FlexVol , questa è la velocità effettiva del volume, misurata in megabyte al secondo. Per i volumi FlexGroup , questa è la somma di MB/s per tutti i volumi costituenti.
- Campi capacità: capacità libera e totale in GiB.

Per maggiori informazioni consultare i seguenti ["Assegnazione di criteri di soglia delle prestazioni agli oggetti di archiviazione"](#)

* ["Rimozione dei criteri di soglia delle prestazioni dagli oggetti di archiviazione"](#)

* ["Tipi di carichi di lavoro 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 suddividere i dati nel cloud"](#)

* ["Visualizzazione dei grafici delle prestazioni per confrontare volumi o LUN che si trovano nello stesso gruppo di policy QoS"](#)

Prestazioni: visualizzazione di tutti gli aggregati

La vista Prestazioni: tutti gli aggregati mostra una panoramica degli eventi di prestazioni, dei dati e delle informazioni di configurazione per ciascun aggregato monitorato da un'istanza di Unified Manager. Questa pagina consente di monitorare le prestazioni dei tuoi aggregati e di risolvere problemi di prestazioni ed eventi di soglia.

Di seguito sono riportati alcuni campi importanti nella vista Prestazioni: Tutti gli aggregati.

- Tipo: Il tipo di aggregato:
 - Disco rigido
 - Ibrido. Combina HDD e SSD, ma Flash Pool non è stato abilitato.

- Ibrido (Flash Pool). Combina HDD e SSD e Flash Pool è stato abilitato.
- SSD
- SSD (FabricPool). Combina SSD e un livello cloud
- HDD (FabricPool). Combina HDD e un livello cloud
- VMDisk (SDS). Dischi virtuali all'interno di una macchina virtuale
- VMDisk (FabricPool). Combina dischi virtuali e un livello cloud
- LUN (FlexArray)
- Segnalazione dati inattivi: indica se la funzionalità di segnalazione dati inattivi è abilitata o disabilitata su questo aggregato. Se abilitata, i volumi di questo aggregato visualizzano la quantità di dati inattivi nella vista Prestazioni: Tutti i volumi. Il valore in questo campo è "N/D" quando la versione di ONTAP non supporta la segnalazione dei dati inattivi.
- Criterio di soglia: il criterio o i criteri di soglia delle prestazioni definiti dall'utente attivi su questo oggetto di archiviazione. È possibile posizionare il cursore sui nomi delle policy contenenti puntini di sospensione (...) per visualizzare il nome completo della policy o l'elenco dei nomi delle policy assegnati. I pulsanti Assegna criterio soglia prestazioni e Cancella criterio soglia prestazioni rimangono disabilitati finché non si selezionano uno o più oggetti facendo clic sulle caselle di controllo situate all'estrema sinistra. Per maggiori informazioni consultare i seguenti ["Assegnazione di criteri di soglia delle prestazioni agli oggetti di archiviazione"](#)
- ["Rimozione dei criteri di soglia delle prestazioni dagli oggetti di archiviazione"](#)

Prestazioni: visualizzazione di tutti i nodi

La vista Prestazioni: tutti i nodi mostra una panoramica degli eventi relativi alle prestazioni, dei dati e delle informazioni di configurazione per ciascun nodo monitorato da un'istanza di Unified Manager. Ciò consente di monitorare rapidamente le prestazioni dei nodi e di risolvere i problemi di prestazioni e gli eventi di soglia.



Flash Cache Reads restituisce la percentuale di operazioni di lettura sul nodo soddisfatte dalla cache, anziché essere restituite dal disco. I dati della Flash Cache vengono visualizzati solo per i nodi e solo quando nel nodo è installato un modulo Flash Cache.

Nel menu **Report**, l'opzione **Report inventario hardware** è disponibile quando Unified Manager e i cluster da esso gestiti sono installati in un sito senza connettività di rete esterna. Questo pulsante genera un file .csv contenente un elenco completo delle informazioni sui cluster e sui nodi, come numeri di modello e numeri di serie dell'hardware, tipi e conteggi dei dischi, licenze installate e altro ancora. Questa funzionalità di reporting è utile per il rinnovo dei contratti all'interno di siti sicuri che non sono connessi alla piattaforma NetApp Active IQ. È possibile assegnare o cancellare criteri di soglia delle prestazioni a qualsiasi oggetto nelle pagine dell'inventario degli oggetti utilizzando i pulsanti **Assegna criterio di soglia delle prestazioni** e **Cancella criterio di soglia delle prestazioni**.

Per maggiori informazioni consultare i seguenti ["Assegnazione di criteri di soglia delle prestazioni agli oggetti di archiviazione"](#)

* ["Rimozione dei criteri di soglia delle prestazioni dagli oggetti di archiviazione"](#)

* ["Generazione di un report di inventario hardware per il rinnovo del contratto"](#)

Prestazioni: visualizzazione di tutte le VM di archiviazione

La vista Prestazioni: tutte le VM di storage mostra una panoramica degli eventi relativi alle prestazioni, dei dati e delle informazioni di configurazione per ciascuna macchina virtuale di storage (SVM) monitorata da un'istanza di Unified Manager. Ciò consente di monitorare rapidamente le prestazioni delle SVM e di risolvere problemi di prestazioni ed eventi di soglia. Il campo Latenza in questa pagina riporta il tempo medio di risposta

per tutte le richieste di I/O, espresso in millisecondi per operazione.



Gli SVM elencati in questa pagina includono solo gli SVM Data e Cluster. Unified Manager non utilizza né visualizza le SVM di amministrazione o di nodo.

Per maggiori informazioni consultare i seguenti ["Assegnazione di criteri di soglia delle prestazioni agli oggetti di archiviazione"](#)

* ["Rimozione dei criteri di soglia delle prestazioni dagli oggetti di archiviazione"](#)

Prestazioni: visualizzazione di tutti i LUN

La vista Prestazioni: tutte le LUN mostra una panoramica degli eventi relativi alle prestazioni, dei dati e delle informazioni di configurazione per ciascuna LUN monitorata da un'istanza di Unified Manager. Ciò consente di monitorare rapidamente le prestazioni dei LUN e di risolvere problemi di prestazioni ed eventi di soglia.

Se vuoi analizzare la latenza e la produttività di un oggetto specifico, fai clic sull'icona Altro  , quindi **Analizza carico di lavoro** e potrai visualizzare grafici di prestazioni e capacità nella pagina **Analisi del carico di lavoro**.

Per maggiori informazioni consultare i seguenti ["Monitoraggio delle LUN in una relazione di gruppo di coerenza"](#)

* ["Provisioning di LUN"](#)

* ["Assegnazione di criteri di soglia delle prestazioni agli oggetti di archiviazione"](#)

* ["Rimozione dei criteri di soglia delle prestazioni dagli oggetti di archiviazione"](#)

* ["Visualizzazione di volumi o LUN che si trovano nello stesso gruppo di policy QoS"](#).

* ["Visualizzazione delle impostazioni del gruppo di criteri QoS applicate a volumi o LUN specifici"](#)

* ["Provisioning di LUN tramite API"](#)

Prestazioni: visualizzazione di tutti gli spazi dei nomi NVMe

La vista Prestazioni: tutti gli spazi dei nomi NVMe mostra una panoramica degli eventi relativi alle prestazioni, 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 prestazioni e lo stato di salute dei tuoi Namespace e di risolvere problemi ed eventi di soglia.

Tra le altre informazioni, vengono riportate le seguenti: Lo stato attuale dello spazio dei nomi. * Offline: l'accesso in lettura o scrittura allo spazio dei nomi non è consentito. * Online - È consentito l'accesso in lettura e scrittura allo spazio dei nomi. * NVFail - Lo spazio dei nomi è stato automaticamente portato offline a causa di un errore NVRAM. * Errore di spazio: lo spazio nello spazio dei nomi è esaurito.

Per maggiori informazioni consultare i seguenti ["Assegnazione di criteri di soglia delle prestazioni agli oggetti di archiviazione"](#)

* ["Rimozione dei criteri di soglia delle prestazioni dagli oggetti di archiviazione"](#)

Prestazioni: visualizzazione di tutte le interfacce di rete

La vista Prestazioni: tutte le interfacce di rete mostra una panoramica degli eventi relativi alle prestazioni, 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 prestazioni delle interfacce e di risolvere i problemi di prestazioni e gli eventi di soglia. Di seguito sono riportati alcuni campi importanti nella vista Prestazioni: tutte le interfacce di rete.

- IOPS: operazioni di input/output al secondo. IOPS non è applicabile ai LIF NFS e ai LIF CIFS e per questi tipi viene visualizzato come N/D.

- Latenza: tempo medio di risposta per tutte le richieste di I/O, espresso in millisecondi per operazione. La latenza non è applicabile ai LIF NFS e ai LIF CIFS e per questi tipi viene visualizzata come N/D.
- Posizione iniziale: la posizione iniziale dell'interfaccia, visualizzata come nome del nodo e nome della porta, separati da due punti (:). Se la posizione viene visualizzata con dei puntini di sospensione (...), puoi posizionare il cursore sul nome della posizione per visualizzarla per intero.
- Posizione corrente: la posizione corrente dell'interfaccia, visualizzata come nome del nodo e nome della porta, separati da due punti (:). Se la posizione viene visualizzata con dei puntini di sospensione (...), puoi posizionare il cursore sul nome della posizione per visualizzarla per intero.
- Ruolo: ruolo dell'interfaccia: dati, cluster, gestione nodi o intercluster.



Le interfacce elencate in questa pagina includono LIF dati, LIF cluster, LIF gestione nodi e LIF intercluster. Unified Manager non utilizza né visualizza i LIF di sistema.

Prestazioni: visualizzazione di tutte le porte

La vista Prestazioni: tutte le porte mostra una panoramica degli eventi relativi alle prestazioni, dei dati e delle informazioni di configurazione per ciascuna porta monitorata da un'istanza di Unified Manager. Ciò consente di monitorare rapidamente le prestazioni delle porte e di risolvere problemi di prestazioni ed eventi di soglia. Per un ruolo di porta, viene visualizzata la funzione della porta di rete: Dati o Cluster. Le porte FCP non possono avere un ruolo e il ruolo viene visualizzato come N/D.



I valori del contatore delle prestazioni vengono visualizzati solo per le porte fisiche. I valori dei contatori non vengono visualizzati per le VLAN o i gruppi di interfacce.

Per maggiori informazioni consultare i seguenti ["Assegnazione di criteri di soglia delle prestazioni agli oggetti di archiviazione"](#)

* ["Rimozione dei criteri di soglia delle prestazioni dagli oggetti di archiviazione"](#)

Prestazioni: visualizzazione Gruppi di criteri QoS

La vista Gruppi di policy QoS mostra i gruppi di policy QoS disponibili nei cluster monitorati da Unified Manager. Ciò include policy QoS tradizionali, policy QoS adattive e policy QoS assegnate tramite livelli di servizio delle prestazioni.

Di seguito sono riportati alcuni campi importanti nella vista Prestazioni: Gruppi di criteri QoS.

- Gruppo di criteri QoS: nome del gruppo di criteri QoS. Per le policy NetApp Service Level Manager (NSLM) 1.3 importate in Unified Manager 9.7 o versioni successive, il nome visualizzato qui include il nome SVM e altre informazioni non presenti nel nome quando è stato definito Performance Service Level in NSLM. Ad esempio, il nome "NSLM_vs6_Performance_2_0" significa 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 archiviazione (SVM) a cui appartiene il gruppo di policy QoS. È possibile fare clic sul nome della VM di archiviazione per accedere alla pagina dei dettagli della VM di archiviazione. Si noti che questo campo è vuoto se il criterio QoS è stato creato sulla VM di archiviazione amministrativa, poiché questo tipo di VM di archiviazione rappresenta il cluster.
- Throughput minimo: il throughput minimo, in IOPS, che il gruppo di policy è tenuto a fornire. Per i criteri adattivi, si tratta del numero minimo di IOPS previsto per TB allocato al volume o LUN, in base alle dimensioni allocate all'oggetto di archiviazione.
- Velocità massima: la velocità massima, in IOPS e/o MB/s, che il gruppo di policy non deve superare. Quando questo campo è vuoto significa che la lunghezza massima definita in ONTAP è infinita. Per i criteri adattivi, questo è il massimo (picco) possibile IOPS per TB allocato al volume o LUN, in base alla

dimensione allocata all'oggetto di archiviazione o alla dimensione utilizzata per l'oggetto di archiviazione.

- IOPS minimo assoluto: per i criteri adattivi, questo è il valore IOPS minimo assoluto utilizzato come override quando gli IOPS previsti sono inferiori a questo valore.
- Dimensione del blocco: la dimensione del blocco specificata per la policy adattiva QoS.
- Assegnazione minima: se per determinare la velocità massima (picco) IOPS viene utilizzato lo "spazio allocato" o lo "spazio utilizzato".
- Latenza prevista: latenza media prevista per le operazioni di input/output dell'archiviazione.
- Condiviso: per le policy QoS tradizionali, indica se i valori di throughput definiti nel gruppo di policy sono condivisi tra più oggetti.
- Oggetti associati: numero di carichi di lavoro assegnati al gruppo di policy QoS. Puoi cliccare sul pulsante Espandi (▼) accanto al nome del gruppo di policy QoS per visualizzare maggiori dettagli sul gruppo di policy.
- Capacità allocata: quantità di spazio attualmente utilizzata dagli oggetti presenti nel gruppo di policy QoS.
- Oggetti associati: numero di carichi di lavoro assegnati al gruppo di policy QoS, separati in volumi e LUN. È possibile fare clic sul numero per passare a una pagina che fornisce maggiori dettagli sui volumi o LUN selezionati.

Per maggiori informazioni consultare gli argomenti sotto ["Gestione delle prestazioni mediante le informazioni del gruppo di policy QoS"](#).

Contenuto della pagina dell'inventario delle prestazioni di raffinazione

Le pagine di inventario per gli oggetti di prestazione 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 dell'inventario degli oggetti Performance possono essere molto estese e spesso occupano più pagine. Questo tipo di dati completi è ottimo per monitorare, tracciare e migliorare le prestazioni; tuttavia, per individuare dati specifici sono necessari strumenti che consentano di individuare rapidamente i dati che si stanno cercando. Pertanto, le pagine dell'inventario degli oggetti Performance contengono funzionalità per la ricerca, l'ordinamento e il filtraggio. Inoltre, la ricerca e il filtraggio possono interagire tra loro per restringere ulteriormente i risultati.

Cerca nelle pagine delle prestazioni dell'inventario degli oggetti

È possibile cercare stringhe nelle pagine Prestazioni inventario oggetti. Utilizzare il campo **Cerca** situato in alto a destra della pagina per individuare rapidamente i dati in base al nome dell'oggetto o al nome della policy. Ciò consente di individuare rapidamente oggetti specifici e i dati associati oppure di individuare rapidamente policy e visualizzare i dati degli oggetti policy associati.

Fare un passo

1. Esegui una delle seguenti opzioni, in base alle tue esigenze di ricerca:

Per localizzare questo...	Scrivi questo...
Un oggetto specifico	Inserisci il nome dell'oggetto nel campo Cerca e clicca su Cerca . Vengono visualizzati l'oggetto cercato e i dati correlati.
Una politica di soglia delle prestazioni definita dall'utente	Inserisci tutto o parte del nome della policy nel campo Cerca e clicca su Cerca . Vengono visualizzati gli oggetti assegnati alla policy ricercata.

Ordina nelle pagine Prestazioni inventario oggetti

È possibile ordinare tutti i dati nelle pagine Prestazioni inventario oggetti in base a qualsiasi colonna, in ordine crescente o decrescente. Ciò consente di individuare rapidamente i dati di inventario degli oggetti, il che è 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 freccia che indica la direzione di ordinamento a destra del nome. Una freccia rivolta verso l'alto indica l'ordine crescente; una freccia rivolta verso il basso indica l'ordine decrescente. L'ordinamento predefinito è in base allo **Stato** (criticità dell'evento) in ordine decrescente, con gli eventi di prestazioni più critici elencati per primi.

Fare un passo

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 Prestazioni inventario oggetti vengono ordinati in ordine crescente o decrescente, in base alla colonna selezionata.

Filtra i dati nelle pagine Prestazioni inventario oggetti

È possibile filtrare i dati nelle pagine Prestazioni inventario oggetti per individuare rapidamente i dati in base a criteri specifici. È possibile utilizzare il filtro per restringere il contenuto delle pagine Prestazioni inventario oggetti in modo da visualizzare solo i risultati specificati. Questo fornisce un metodo molto efficiente per visualizzare solo i dati sulle prestazioni a cui sei interessato.

Puoi utilizzare il pannello Filtraggio per personalizzare la visualizzazione della griglia in base alle tue preferenze. Le opzioni di filtro disponibili si basano sul tipo di oggetto visualizzato nella griglia. Se sono attualmente applicati dei filtri, il numero di filtri applicati viene visualizzato a destra del pulsante Filtro.

Sono supportati tre tipi di parametri di filtro.

Parametro	Validazione
Stringa (testo)	Gli operatori sono contiene , inizia con , termina con e non contiene .

Parametro	Validazione
Numero	Gli operatori sono maggiore di , minore di , nell'ultimo e tra .
Enum (testo)	Gli operatori sono is e is not .

I campi Colonna, Operatore e Valore sono obbligatori per ciascun filtro; i filtri disponibili riflettono le colonne filtrabili nella pagina corrente. Il numero massimo di filtri che puoi 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 Filtraggio.

1. Nella parte superiore della pagina, fare clic sul pulsante **Filtro**. Viene visualizzato il pannello 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, seleziona o immetti un valore per completare il filtro per quell'oggetto.
5. Per aggiungere un altro filtro, fare clic su **+Aggiungi filtro**. Viene visualizzato un campo filtro aggiuntivo. Completare questo filtro utilizzando la procedura descritta nei passaggi precedenti. Tieni presente che dopo aver aggiunto il quarto filtro, il pulsante **+Aggiungi filtro** non verrà 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 Filtro.
7. Utilizzare il pannello Filtraggio per rimuovere singoli filtri facendo clic sull'icona del cestino a destra del filtro da rimuovere.
8. Per rimuovere tutti i filtri, fare clic su **Reimposta** nella parte inferiore del pannello di filtraggio.

Esempio di filtraggio

L'illustrazione mostra il pannello Filtraggio con tre filtri. Il pulsante **+Aggiungi filtro** viene visualizzato quando si hanno meno del massimo di quattro filtri.

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

Dopo aver cliccato su **Applica filtro**, il pannello Filtraggio si chiude, applica i filtri e mostra il numero di filtri applicati ().

Comprendere le raccomandazioni di Unified Manager per suddividere i dati nel cloud

La vista Prestazioni: tutti i volumi mostra informazioni relative alle dimensioni dei dati utente archiviati sul volume inattivo (freddo). In alcuni casi, Unified Manager identifica determinati volumi che trarrebbero vantaggio dall'organizzazione dei dati inattivi nel livello cloud (provider cloud o StorageGRID) di un aggregato abilitato per 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 di suddividere i dati in livelli richiede l'aggiornamento del software ONTAP. Inoltre, il **auto** La politica di suddivisione in livelli è stata introdotta in ONTAP 9.4 e **all** La politica di suddivisione in livelli è stata introdotta in ONTAP 9.6, quindi se si consiglia di utilizzare la politica di suddivisione in livelli automatica, è necessario eseguire l'aggiornamento a ONTAP 9.4 o versione successiva.

I tre campi seguenti nella vista Prestazioni: Tutti i volumi forniscono informazioni sulla possibilità di migliorare l'utilizzo del disco del sistema di archiviazione e di risparmiare spazio sul livello delle prestazioni spostando i dati inattivi sul livello cloud.

- **Politica di suddivisione in livelli**

La politica di suddivisione in livelli determina se i dati sul volume rimangono sul livello delle prestazioni o se alcuni dati vengono spostati dal livello delle prestazioni al livello cloud.

Il valore in questo campo indica la politica di suddivisione in livelli impostata sul volume, anche se il volume non risiede attualmente su un aggregato FabricPool. La politica di suddivisione in livelli ha effetto solo quando il volume si trova su un aggregato FabricPool.

- **Dati inespressi**

I dati freddi mostrano la dimensione dei dati utente memorizzati sul volume inattivo (freddo).

Un valore viene visualizzato qui solo quando si utilizza il software ONTAP 9.4 o versione successiva perché richiede che l'aggregato su cui viene distribuito il volume abbia **inactive data reporting parameter** impostato su **enabled**, e che sia stata raggiunta la soglia minima di giorni di raffreddamento (per i volumi che utilizzano il **snapshot-only** o **auto** politica di livelli). In caso contrario il valore è indicato come "N/D".

- **Raccomandazione cloud**

Dopo aver acquisito informazioni sufficienti sull'attività dei dati sul volume, Unified Manager potrebbe stabilire che non è richiesta alcuna azione oppure che è possibile risparmiare spazio sul livello delle prestazioni suddividendo i dati inattivi nel livello cloud.



Il campo Cold Data viene aggiornato ogni 15 minuti, ma il campo Cloud Recommendation viene aggiornato ogni 7 giorni quando l'analisi dei cold data viene eseguita sul volume. Pertanto, la quantità esatta di dati freddi può variare tra i campi. Nel campo Raccomandazione cloud viene visualizzata la data in cui è stata eseguita l'analisi.

Quando la segnalazione dei dati inattivi è abilitata, il campo Dati inattivi visualizza la quantità esatta di dati inattivi. Senza la funzionalità di segnalazione dei dati inattivi, Unified Manager utilizza le statistiche sulle prestazioni per determinare se i dati sono inattivi su un volume. In questo caso, la quantità di dati inattivi non

viene visualizzata nel campo Cold Data, ma viene visualizzata quando si passa il cursore sulla parola **Tier** per visualizzare la raccomandazione cloud.

I consigli sul cloud che vedrai sono:

- **Apprendimento.** Non sono stati raccolti dati sufficienti per formulare una raccomandazione.
- **Livello.** L'analisi ha determinato che il volume contiene dati inattivi (freddi) e che è necessario configurare il volume per spostare tali dati sul livello cloud. In alcuni casi potrebbe essere necessario spostare prima il volume su un aggregato abilitato per FabricPool. Negli altri casi in cui il volume è già su un aggregato FabricPool, è sufficiente modificare la politica di suddivisione in livelli.
- **Nessuna azione.** O il volume contiene pochissimi dati inattivi, oppure è già impostato sul criterio di suddivisione in livelli "auto" su un aggregato FabricPool, oppure 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 per modificare i criteri di suddivisione in livelli del volume o le impostazioni di reporting dei dati inattivi aggregati, utilizzare ONTAP System Manager, i comandi ONTAP CLI o una combinazione di questi strumenti.

Se hai effettuato l'accesso a Unified Manager con il ruolo di Amministratore applicazioni o Amministratore archiviazione, il collegamento **Configura volume** è disponibile nella raccomandazione cloud quando passi il cursore sulla parola **Livello**. Fare clic su questo pulsante per aprire la pagina Volumi in System Manager e apportare la modifica consigliata.

Monitorare le prestazioni utilizzando le pagine di Performance Explorer

Le pagine di Performance Explorer mostrano informazioni dettagliate sulle prestazioni di ciascun oggetto in un cluster. La pagina fornisce una visualizzazione dettagliata delle prestazioni di tutti gli oggetti del cluster, consentendo di selezionare e confrontare i dati sulle prestazioni di oggetti specifici in diversi periodi di tempo.

È inoltre possibile valutare le prestazioni complessive di tutti gli oggetti e confrontare i dati sulle prestazioni degli oggetti in un formato affiancato.

Comprendere l'oggetto radice

L'oggetto radice è la linea di base rispetto alla quale vengono effettuati i confronti con altri oggetti. Ciò consente di visualizzare e confrontare i dati di altri oggetti con l'oggetto radice, fornendo un'analisi dei dati sulle prestazioni che aiuta a risolvere i problemi e a migliorare le prestazioni dell'oggetto.

Il nome dell'oggetto radice viene visualizzato nella parte superiore del riquadro Confronto. Gli oggetti aggiuntivi vengono visualizzati sotto l'oggetto radice. Sebbene non vi sia alcun limite al numero di oggetti aggiuntivi che è possibile aggiungere al riquadro Confronto, è consentito un solo oggetto radice. I dati per l'oggetto radice vengono visualizzati automaticamente nei grafici nel riquadro Grafici contatore.

Non è possibile modificare l'oggetto radice; è sempre impostato sulla pagina dell'oggetto che si sta visualizzando. Ad esempio, se si apre la pagina Volume Performance Explorer di Volume1, Volume1 è l'oggetto radice e non può essere modificato. Se vuoi effettuare un confronto con un oggetto radice diverso, devi cliccare sul collegamento di un oggetto e aprire la relativa landing page.



Gli eventi e le soglie vengono visualizzati solo per gli oggetti radice.

Applica il filtro per ridurre l'elenco degli oggetti correlati nella griglia

Il filtraggio consente di visualizzare un sottoinsieme di oggetti più piccolo e meglio definito nella griglia. Ad esempio, se nella griglia sono presenti 25 volumi, il filtraggio consente di visualizzare solo i volumi con una velocità effettiva inferiore a 90 MBps o una latenza superiore a 1 ms/op.

Specificare un intervallo di tempo per gli oggetti correlati

Il selettore Intervallo di tempo nella pagina Esplora prestazioni consente di specificare l'intervallo di tempo per il confronto dei dati degli oggetti. Specificando un intervallo di tempo, il contenuto delle pagine di Performance Explorer viene perfezionato in modo da visualizzare solo i dati degli oggetti compresi nell'intervallo di tempo specificato.

L'ottimizzazione dell'intervallo di tempo rappresenta un metodo efficiente per visualizzare solo i dati sulle prestazioni a cui si è interessati. È possibile selezionare un intervallo di tempo predefinito oppure specificarne uno personalizzato. L'intervallo di tempo predefinito è costituito dalle 72 ore precedenti.

Seleziona un intervallo di tempo predefinito

La selezione di un intervallo di tempo predefinito è un modo rapido ed efficiente per personalizzare e focalizzare l'output dei dati quando si visualizzano i dati sulle prestazioni degli oggetti cluster. Selezionando un intervallo di tempo predefinito, sono disponibili dati fino a 13 mesi.

Passi

1. In alto a destra della pagina **Performance Explorer**, fare clic su **Intervallo di tempo**.
2. Dal lato destro del pannello **Selezione intervallo di tempo**, seleziona un intervallo di tempo predefinito.
3. Fare clic su **Applica intervallo**.

Specificare un intervallo di tempo personalizzato

La pagina Performance Explorer consente di specificare l'intervallo di data e ora per i dati sulle prestazioni. Specificare un intervallo di tempo personalizzato garantisce una maggiore flessibilità rispetto all'utilizzo di intervalli di tempo predefiniti durante l'elaborazione dei dati degli oggetti cluster.

È possibile selezionare un intervallo di tempo compreso tra un'ora e 390 giorni. 13 mesi equivalgono a 390 giorni perché ogni mese viene conteggiato come 30 giorni. Specificando un intervallo di data e ora si ottengono maggiori dettagli e si può dare un'occhiata più da vicino a specifici eventi o serie di eventi. Specificare un intervallo di tempo aiuta anche a risolvere potenziali problemi di prestazioni, poiché specificando un intervallo di data e ora vengono visualizzati i dati relativi all'evento di prestazioni in modo più dettagliato. Utilizzare il controllo **Intervallo di tempo** per selezionare intervalli di data e ora predefiniti oppure specificare un intervallo di data e ora personalizzato fino a 390 giorni. I pulsanti per gli 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 che avvisa che i dati sulle prestazioni visualizzati per un periodo superiore a 30 giorni vengono rappresentati graficamente utilizzando medie orarie e non un polling di dati di 5 minuti. Potrebbe quindi verificarsi una perdita di granularità visiva della sequenza temporale. Se si fa clic sull'opzione **Non mostrare più** nella finestra di dialogo, il messaggio non verrà visualizzato quando si seleziona l'opzione **Ultimi 13 mesi** o si specifica un intervallo di date personalizzato superiore a 30 giorni. I dati riepilogativi si applicano anche a un intervallo di tempo più piccolo, se l'intervallo di tempo include un'ora/data che è superiore a 30 giorni a partire da oggi.

Quando si seleziona un intervallo di tempo (personalizzato o predefinito), gli intervalli di tempo pari o inferiori a 30 giorni si basano su campioni di dati con intervalli di 5 minuti. Gli intervalli di tempo superiori a 30 giorni si basano su campioni di dati con 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**. Selezionando un intervallo di tempo predefinito, sono disponibili dati fino a 13 mesi. Il pulsante dell'intervallo di tempo predefinito selezionato viene evidenziato e i giorni e gli orari corrispondenti vengono visualizzati nei calendari e nei selettori di orario.
3. Per selezionare un intervallo di date personalizzato, fare clic sulla data di inizio nel calendario **Da** a sinistra. Fare clic su **<** o **>** per navigare avanti o indietro nel calendario. Per specificare la data di fine, fare clic su una data nel calendario **A** sulla destra. Tieni presente che la data di fine predefinita è oggi, a meno che tu non ne specifichi una diversa. Il pulsante **Intervallo personalizzato** a destra del pannello Intervallo di tempo è evidenziato, a indicare che hai selezionato un intervallo di date personalizzato.
4. Per selezionare un intervallo di tempo personalizzato, fare clic sul controllo **Ora** sotto il calendario **Da** e selezionare l'ora di inizio. Per specificare l'ora di fine, fare clic sul controllo **Ora** sotto il calendario **A** sulla destra e selezionare l'ora di fine. Il pulsante **Intervallo personalizzato** a destra del pannello 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 gli orari di inizio e fine come descritto in precedenza. Le date selezionate vengono evidenziate nei calendari, gli orari di inizio e fine specificati vengono visualizzati nei controlli **Ora** e il pulsante **Intervallo personalizzato** viene evidenziato.
6. Dopo aver selezionato l'intervallo di data e ora, fare clic su **Applica intervallo**. Le statistiche sulle prestazioni per quell'intervallo di tempo vengono visualizzate nei grafici e nella cronologia degli eventi.

Definire l'elenco degli oggetti correlati per la creazione di grafici di confronto

È possibile definire un elenco di oggetti correlati per il confronto di dati e prestazioni nel riquadro Grafico contatore. Ad esempio, se la macchina virtuale di archiviazione (SVM) riscontra un problema di prestazioni, è possibile confrontare tutti i volumi nella SVM per identificare quale volume potrebbe causare il problema.

È possibile aggiungere qualsiasi oggetto nella griglia degli oggetti correlati ai riquadri Grafico di confronto e Grafico contatore. Ciò consente di visualizzare e confrontare i dati di più oggetti e con l'oggetto radice. È possibile aggiungere e rimuovere oggetti dalla griglia degli oggetti correlati; tuttavia, l'oggetto radice nel riquadro Confronto non è rimovibile.



L'aggiunta di molti oggetti al riquadro Confronto potrebbe avere un impatto negativo sulle prestazioni. Per mantenere le prestazioni, è consigliabile selezionare un numero limitato di grafici per il confronto dei dati.

Passi

1. Nella griglia degli oggetti, individua l'oggetto che desideri aggiungere e fai clic sul pulsante **Aggiungi**.

Il pulsante **Aggiungi** diventa grigio e l'oggetto viene aggiunto all'elenco degli oggetti aggiuntivi nel riquadro Confronto. I dati dell'oggetto vengono aggiunti ai grafici nei riquadri Grafici contatore. Il colore dell'icona dell'occhio dell'oggetto () corrisponde al colore della linea di tendenza dei dati dell'oggetto nei grafici.

2. **Facoltativo:** Nascondi o mostra i dati per gli oggetti selezionati:

Per fare questo...	Intraprendi questa azione...
Nascondi un oggetto selezionato	Fare clic sull'icona dell'occhio dell'oggetto selezionato () nel riquadro Confronto. I dati dell'oggetto vengono nascosti e l'icona a forma di occhio diventa grigia.
Mostra un oggetto nascosto	Fare clic sull'icona a forma di occhio grigio dell'oggetto selezionato nel riquadro Confronto. L'icona dell'occhio torna al suo colore originale e i dati dell'oggetto vengono aggiunti nuovamente ai grafici nel riquadro Grafici contatore.

3. **Facoltativo:** Rimuovi gli oggetti selezionati dal riquadro **Confronto**:

Per fare questo...	Intraprendi questa azione...
Rimuovi un oggetto selezionato	Passare il mouse sul nome dell'oggetto selezionato nel riquadro Confronto per visualizzare il pulsante Rimuovi oggetto (X), quindi fare clic sul pulsante. L'oggetto viene rimosso dal riquadro Confronto e i suoi dati vengono cancellati dai grafici dei contatori.

Per fare questo...	Intraprendi questa azione...
Rimuovi tutti gli oggetti selezionati	Fare clic sul pulsante Rimuovi tutti gli oggetti (X) nella parte superiore del riquadro Confronto. Tutti gli oggetti selezionati e i relativi dati vengono rimossi, lasciando solo l'oggetto radice.

Comprendere i grafici dei contatori

I grafici nel riquadro Grafici contatore consentono di visualizzare e confrontare i dati sulle prestazioni dell'oggetto radice e degli oggetti aggiunti dalla griglia degli oggetti correlati. Ciò può aiutarti a comprendere le tendenze delle prestazioni e a isolare e risolvere i problemi di prestazioni.

I grafici dei contatori visualizzati per impostazione predefinita sono Eventi, Latenza, IOPS e MBps. I grafici facoltativi che puoi scegliere di visualizzare sono Utilizzo, Capacità di prestazioni utilizzata, IOPS disponibili, IOPS/TB e Rapporto di mancata memorizzazione nella cache. Inoltre, è possibile scegliere di visualizzare i valori totali o i valori di ripartizione per i grafici Latenza, IOPS, MBps e Capacità di prestazioni utilizzata.

Per impostazione predefinita, Performance Explorer visualizza determinati grafici dei contatori, indipendentemente dal fatto che l'oggetto di archiviazione li supporti tutti o meno. Quando un contatore non è supportato, il grafico del contatore è vuoto e il messaggio `Not applicable for <object>` viene visualizzato.

I grafici mostrano le tendenze delle prestazioni per l'oggetto radice e per tutti gli oggetti selezionati nel riquadro Confronto. I dati in ogni grafico sono organizzati come segue:

- **asse X**

Visualizza il periodo di tempo specificato. Se non hai specificato un intervallo di tempo, l'impostazione predefinita è il periodo di 72 ore precedente.

- **Asse Y**

Visualizza le unità di misura specifiche dell'oggetto o degli oggetti selezionati.

I colori delle linee di tendenza corrispondono al colore del nome dell'oggetto visualizzato nel riquadro Confronto. È possibile posizionare il cursore su un punto di qualsiasi linea di tendenza per visualizzare i dettagli relativi a tempo e valore per quel punto.

Se si desidera analizzare un periodo di tempo specifico all'interno di un grafico, è possibile utilizzare uno dei seguenti metodi:

- Utilizzare il pulsante **<** per espandere il riquadro Grafici contatore in modo che copra l'intera larghezza della pagina.
- Utilizzare il cursore (quando si trasforma in una lente di ingrandimento) per selezionare una porzione dell'intervallo di tempo nel grafico per mettere a fuoco e ingrandire quell'area. È possibile fare clic su Reimposta zoom grafico per riportare il grafico all'intervallo di tempo predefinito.
- Utilizzare il pulsante **Zoom vista** per visualizzare un grande grafico a contatore singolo contenente dettagli estesi e indicatori di soglia.



Occasionalmente si verificano delle lacune nelle linee di tendenza. Le lacune indicano che Unified Manager non è riuscito a raccogliere i dati sulle prestazioni dal sistema di archiviazione oppure che Unified Manager potrebbe essere inattivo.

Tipi di grafici contatori delle prestazioni

Sono disponibili grafici delle prestazioni standard che visualizzano i valori del contatore per l'oggetto di archiviazione selezionato. Ciascuno dei grafici dei contatori di ripartizione mostra i valori totali suddivisi in lettura, scrittura e altre categorie. Inoltre, alcuni grafici del contatore di ripartizione mostrano dettagli aggiuntivi quando il grafico è visualizzato in modalità Zoom.

Nella tabella seguente sono riportati i grafici dei contatori delle prestazioni disponibili.

Grafici disponibili	Descrizione del grafico
Eventi	Visualizza eventi critici, di errore, di avviso e informativi in correlazione con i grafici statistici per l'oggetto radice. Gli eventi sanitari vengono visualizzati in aggiunta agli eventi prestazionali per fornire un quadro completo dei motivi per cui le prestazioni potrebbero essere compromesse.
Latenza - Totale	Numero di millisecondi necessari per rispondere alle richieste dell'applicazione. Si noti che i valori di latenza media sono ponderati in base all'I/O.
Latenza - Ripartizione	Le stesse informazioni mostrate in Latenza totale, ma con i dati sulle prestazioni separati in lettura, scrittura e altra latenza. Questa opzione del grafico si applica solo quando l'oggetto selezionato è un SVM, un nodo, un aggregato, un volume, un LUN o uno spazio dei nomi.
Latenza - Componenti del cluster	Le stesse informazioni sono mostrate in Latenza totale, ma con i dati sulle prestazioni separati in base alla latenza per componente del cluster. Questa opzione del 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 "Totale" vengono visualizzati gli IOPS per i dati che si spostano attraverso questo nodo e che possono risiedere sul nodo locale o remoto, mentre selezionando "Totale (Locale)" vengono visualizzati gli IOPS per i dati che risiedono solo sul nodo corrente.

Grafici disponibili	Descrizione del grafico
IOPS - Ripartizione	Le stesse informazioni mostrate in IOPS Total, ma con i dati sulle prestazioni separati in lettura, scrittura e altri IOPS. Questa opzione del grafico si applica solo quando l'oggetto selezionato è un SVM, un nodo, un aggregato, un volume, un LUN o uno spazio dei nomi. Quando visualizzato nella vista Zoom, il grafico dei volumi mostra i valori minimi e massimi della velocità effettiva QoS, se configurati in ONTAP. Quando viene visualizzato per un nodo, selezionando "Breakdown" viene visualizzata la ripartizione IOPS per i dati che si spostano attraverso questo nodo e che possono risiedere sul nodo locale o remoto, mentre selezionando "Breakdown (Locale)" viene visualizzata la ripartizione IOPS per i dati che risiedono solo sul nodo corrente.
IOPS - Protocolli	Le stesse informazioni sono mostrate in IOPS Total, ma i dati sulle prestazioni sono separati in grafici individuali per il traffico dei protocolli CIFS, NFS, FCP, NVMe e iSCSI. Questa opzione del grafico si applica solo quando l'oggetto selezionato è un 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. Chiamato anche densità I/O, questo contatore misura la quantità di prestazioni che può essere fornita da una determinata quantità di capacità di archiviazione. Quando visualizzato nella vista Zoom, il grafico dei volumi mostra i valori previsti di QoS e di throughput di picco, se configurati in ONTAP. Questa opzione del 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.

Grafici disponibili	Descrizione del grafico
MB/s - Ripartizione	Le informazioni sono le stesse mostrate nel grafico MB/s, ma con i dati di throughput separati in letture del disco, letture della cache Flash, scritture e altro. Quando visualizzato nella vista Zoom, il grafico dei volumi mostra i valori massimi di throughput QoS, se configurati in ONTAP. Questa opzione del grafico si applica solo quando l'oggetto selezionato è un SVM, un nodo, un aggregato, un volume, un LUN o uno spazio dei nomi.  I dati della Flash Cache vengono visualizzati solo per i nodi e solo quando nel nodo è installato un modulo Flash Cache.
Capacità di prestazione utilizzata - Totale	Percentuale della capacità di prestazione consumata dal nodo o dall'aggregato.
Capacità di prestazione utilizzata - Ripartizione	Capacità di prestazione Dati utilizzati separati in protocolli utente e processi in background del sistema. Inoltre, viene mostrata la quantità di capacità di prestazione libera.
IOPS disponibili - Totale	Numero di operazioni di input/output al secondo attualmente disponibili (gratuite) su questo oggetto. Questo numero è il risultato della sottrazione degli IOPS attualmente utilizzati dagli IOPS totali che Unified Manager calcola che l'oggetto può eseguire. Questa opzione del grafico si applica solo quando l'oggetto selezionato è un nodo o un aggregato.
Utilizzo - Totale	Percentuale di risorse disponibili dell'oggetto in uso. L'utilizzo indica l'utilizzo dei nodi per i nodi, l'utilizzo dei dischi per gli aggregati e l'utilizzo della larghezza di banda per le porte. Questa opzione del grafico si applica solo quando l'oggetto selezionato è un nodo, un aggregato o una porta.
Rapporto di mancata visualizzazione della cache - Totale	Percentuale di richieste di lettura da applicazioni client restituite dal disco anziché dalla cache. Questa opzione del grafico si applica solo quando l'oggetto selezionato è un volume.

Seleziona i 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 Grafici dei contatori. Ciò consente di visualizzare

dati e contatori specifici, in base ai requisiti di prestazioni.

Passi

- 1. Nel riquadro **Grafici contatore**, fare clic sull'elenco a discesa **Scegli grafici**.
- 2. Aggiungere o rimuovere grafici:

A...	Fai questo...
Aggiungere o rimuovere singoli grafici	Fai clic sulle caselle di controllo accanto ai grafici che desideri mostrare o nascondere
Aggiungi tutti i grafici	Fai clic su Seleziona tutto
Rimuovi tutti i grafici	Fai clic su Deseleziona tutto

Le selezioni del grafico vengono visualizzate nel riquadro Grafici contatore. Tieni presente che quando aggiungi grafici, i nuovi grafici vengono inseriti nel riquadro Grafici contatore in modo che corrispondano all'ordine dei grafici elencati nell'elenco a discesa Scegli grafici. La selezione di grafici aggiuntivi potrebbe richiedere uno scorrimento aggiuntivo.

Espandi il riquadro Grafici contatore

È possibile espandere il riquadro Grafici contatore 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 Grafici contatori più grande. Per espandere il riquadro, utilizzare il pulsante < al centro della finestra Performance Explorer.

Fare un passo

- 1. Espandi o riduci il riquadro **Grafici dei contatori**.

A...	Fai questo...
Espandi il riquadro Grafici contatore per adattarlo alla larghezza della pagina	Fare clic sul pulsante <
Ridurre il riquadro Grafici contatore nella metà destra della pagina	Fare clic sul pulsante >

Cambia il focus dei grafici dei contatori in un periodo di tempo più breve

È possibile utilizzare il mouse per ridurre l'intervallo di tempo e concentrarsi su un periodo di tempo specifico nel riquadro Grafico contatore o nella finestra Visualizzazione zoom dei grafici contatore. Ciò consente di avere una visione più granulare e microscopica di qualsiasi parte della cronologia dei dati sulle prestazioni, degli eventi e delle soglie.

Prima di iniziare

Per indicare che questa funzionalità è attiva, il cursore deve trasformarsi in una lente di ingrandimento.



Quando si utilizza questa funzione, che modifica la sequenza temporale per visualizzare valori che corrispondono alla visualizzazione più granulare, l'intervallo di data e ora nel selettore **Intervallo di tempo** non cambia rispetto ai valori originali del grafico.

Passi

1. Per ingrandire un periodo di tempo specifico, fare clic con la lente di ingrandimento e trascinare il mouse per evidenziare l'area che si desidera visualizzare in dettaglio.

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 **Intervallo di tempo**, fare clic sul pulsante **Reimposta zoom grafico**.

Il grafico del contatore viene visualizzato nel suo stato originale.

Visualizza i 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 a integrità e prestazioni che si sono verificati sull'oggetto radice durante un intervallo di tempo specificato, il che può essere utile per la risoluzione dei problemi di prestazioni.

Il riquadro Cronologia eventi mostra gli eventi critici, di errore, di avviso e informativi che si sono verificati sull'oggetto radice durante l'intervallo di tempo selezionato. Ogni gravità dell'evento ha una propria tempistica. Gli eventi singoli e multipli sono rappresentati da un punto evento sulla sequenza temporale. Puoi posizionare il cursore sul punto di un evento per visualizzarne i dettagli. Per aumentare la granularità visiva di più eventi, è possibile ridurre l'intervallo di tempo. In questo modo più eventi vengono suddivisi in singoli eventi, consentendo di visualizzare e analizzare separatamente ciascun evento.

Ogni punto dell'evento di performance sulla cronologia degli eventi si allinea verticalmente con un picco corrispondente nelle linee di tendenza dei grafici del contatore visualizzate sotto la cronologia degli eventi. Ciò fornisce una correlazione visiva diretta tra gli eventi e le prestazioni complessive. Anche gli eventi sanitari vengono visualizzati sulla cronologia, ma questi tipi di eventi non coincidono necessariamente con un picco in uno dei grafici delle prestazioni.

Passi

1. Nel riquadro **Cronologia eventi**, posizionare il cursore su un punto evento su una cronologia per visualizzare un riepilogo dell'evento o degli eventi in quel punto.

Una finestra di dialogo pop-up mostra 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:

Per fare questo...	Clicca qui...
Visualizza i dettagli di un singolo evento	Visualizza dettagli evento nella finestra di dialogo pop-up.
Visualizza i dettagli per più eventi	Visualizza dettagli evento nella finestra di dialogo pop-up.  Facendo clic su un singolo evento nella finestra di dialogo degli eventi multipli viene visualizzata la pagina Dettagli evento appropriata.

Visualizzazione zoom dei grafici dei contatori

I grafici dei contatori forniscono una vista zoom che consente di ingrandire i dettagli delle prestazioni nel periodo di tempo specificato. Ciò consente di visualizzare i dettagli delle prestazioni e gli eventi con una granularità molto più elevata, il che è utile quando si risolvono problemi di prestazioni.

Quando vengono visualizzati in modalità Zoom, alcuni grafici di ripartizione forniscono informazioni aggiuntive rispetto a quelle visualizzate quando il grafico non è in modalità Zoom. Ad esempio, le pagine Zoom View dei grafici di ripartizione IOPS, IOPS/TB e MBps mostrano i valori dei criteri QoS per volumi e LUN se sono stati impostati in ONTAP.



Per i criteri di soglia delle prestazioni definiti dal sistema, nell'elenco **Criteri** sono disponibili solo i criteri "Risorse nodo sovrautilizzate" e "Limite di throughput QoS violato". Al momento, gli altri criteri di soglia definiti dal sistema non sono disponibili.

Visualizza la vista zoom dei grafici del contatore

La vista zoom dei grafici contatore fornisce un livello di dettaglio più preciso per il grafico contatore selezionato e la relativa cronologia. In questo modo i dati del grafico del contatore vengono ingranditi, consentendo di avere una visione più nitida degli eventi di performance e delle relative cause sottostanti.

È possibile visualizzare la vista zoom dei grafici dei contatori per qualsiasi grafico dei contatori.

Passi

1. Fare clic su **Zoom vista** per aprire il grafico selezionato in una nuova finestra del browser.
2. Se si visualizza un grafico analitico e si fa clic su **Visualizzazione zoom**, il grafico analitico viene visualizzato in visualizzazione zoom. Puoi selezionare **Totale** mentre sei in Visualizzazione zoom se vuoi cambiare l'opzione di visualizzazione.

Specificare l'intervallo di tempo nella vista Zoom

Il controllo **Intervallo di tempo** nella finestra Visualizzazione zoom grafici contatore consente di specificare un intervallo di data e ora per il grafico selezionato. Ciò consente

di 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 equivalgono a 390 giorni perché ogni mese viene conteggiato come 30 giorni. Specificando un intervallo di data e ora si ottengono maggiori dettagli e si può dare un'occhiata più da vicino a specifici eventi o serie di eventi. Specificare un intervallo di tempo aiuta anche a risolvere potenziali problemi di prestazioni, poiché specificando un intervallo di data e ora vengono visualizzati i dati relativi all'evento di prestazioni in modo più dettagliato. Utilizzare il controllo **Intervallo di tempo** per selezionare intervalli di data e ora predefiniti oppure specificare un intervallo di data e ora personalizzato fino a 390 giorni. I pulsanti per gli 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 che avvisa che i dati sulle prestazioni visualizzati per un periodo superiore a 30 giorni vengono rappresentati graficamente utilizzando medie orarie e non un polling di dati di 5 minuti. Potrebbe quindi verificarsi una perdita di granularità visiva della sequenza temporale. Se si fa clic sull'opzione **Non mostrare più** nella finestra di dialogo, il messaggio non verrà visualizzato quando si seleziona l'opzione **Ultimi 13 mesi** o si specifica un intervallo di date personalizzato superiore a 30 giorni. I dati riepilogativi si applicano anche a un intervallo di tempo più piccolo, se l'intervallo di tempo include un'ora/data che è superiore a 30 giorni a partire da oggi.

Quando si seleziona un intervallo di tempo (personalizzato o predefinito), gli intervalli di tempo pari o inferiori a 30 giorni si basano su campioni di dati con intervalli di 5 minuti. Gli intervalli di tempo superiori a 30 giorni si basano su campioni di dati con intervalli di un'ora.

The screenshot shows a 'Time Range' selection interface. It includes two side-by-side calendar grids for April 2015. The left grid, labeled 'From', shows the 12th selected. The right grid, labeled 'To', shows the 15th selected. Below each calendar is a 'Time' dropdown menu, both currently set to '6:00 am'. To the right of the calendars is a vertical list of predefined time range buttons: 'Last Hour', 'Last 24 Hours', 'Last 72 Hours', 'Last 7 Days', 'Last 30 Days', 'Last 13 Months', and 'Custom Range'. At the bottom right of the dialog are 'Cancel' and 'Apply Range' buttons.

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**. Selezionando un intervallo di tempo predefinito, sono disponibili dati fino a 13 mesi. Il pulsante dell'intervallo di tempo predefinito selezionato viene evidenziato e i giorni e gli orari corrispondenti vengono visualizzati nei calendari e nei selettori di orario.
3. Per selezionare un intervallo di date personalizzato, fare clic sulla data di inizio nel calendario **Da** a sinistra. Fare clic su **<** o **>** per navigare avanti o indietro nel calendario. Per specificare la data di fine, fare clic su una data nel calendario **A** sulla destra. Tieni presente che la data di fine predefinita è oggi, a meno che tu non ne specifichi una diversa. Il pulsante **Intervallo personalizzato** a destra del pannello Intervallo di tempo è evidenziato, a indicare che hai selezionato un intervallo di date personalizzato.
4. Per selezionare un intervallo di tempo personalizzato, fare clic sul controllo **Ora** sotto il calendario **Da** e selezionare l'ora di inizio. Per specificare l'ora di fine, fare clic sul controllo **Ora** sotto il calendario **A** sulla destra e selezionare l'ora di fine. Il pulsante **Intervallo personalizzato** a destra del pannello 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 gli orari di inizio e fine come descritto in precedenza. Le date selezionate vengono evidenziate nei calendari, gli orari di inizio e fine specificati vengono visualizzati nei controlli **Ora** e il pulsante **Intervallo personalizzato** viene evidenziato.
6. Dopo aver selezionato l'intervallo di data e ora, fare clic su **Applica intervallo**. Le statistiche sulle prestazioni per quell'intervallo di tempo vengono visualizzate nei grafici e nella cronologia degli eventi.

Seleziona le soglie di prestazione nella vista zoom dei grafici dei contatori

L'applicazione delle soglie nella vista zoom dei grafici dei contatori fornisce una visualizzazione dettagliata delle occorrenze degli eventi di soglia delle prestazioni. Ciò consente di applicare o rimuovere soglie e di visualizzare immediatamente i risultati, il che può essere utile per decidere se la risoluzione dei problemi debba essere il passo successivo.

Selezionando le soglie nella vista zoom dei grafici dei contatori è possibile visualizzare dati precisi sugli eventi di soglia delle prestazioni. È possibile applicare qualsiasi soglia visualizzata nell'area **Politiche** della vista zoom dei grafici dei contatori.

Nella vista zoom dei grafici dei contatori è possibile applicare solo una policy alla volta all'oggetto.

Fare un passo

1. Seleziona o deseleziona il  che è associato a una politica.

La soglia selezionata viene applicata alla vista zoom dei grafici dei contatori. Le soglie critiche sono visualizzate come una linea rossa; le soglie di avviso sono visualizzate come una linea gialla.

Visualizza la latenza del volume per componente del cluster

È possibile visualizzare informazioni dettagliate sulla latenza di un volume utilizzando la pagina Volume Performance Explorer. Il grafico del contatore Latenza - Totale mostra la latenza totale sul volume, mentre il grafico del contatore Latenza - Ripartizione 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 aiutare a determinare in che modo ciascun componente contribuisce alla latenza totale sul volume. Vengono visualizzati i seguenti componenti del cluster:

- Rete
- Limite QoS massimo
- Limite minimo QoS
- Elaborazione di rete
- Interconnessione del cluster
- Data Processing
- Operazioni aggregate

- Attivazione del volume
- Risorse MetroCluster
- Latenza del cloud
- Sincronizza SnapMirror

Passi

1. Nella pagina **Volume Performance Explorer** per il volume selezionato, dal grafico Latenza, seleziona **Componenti cluster** dal menu a discesa.

Viene visualizzato il grafico Latenza - Componenti del cluster.

2. Per visualizzare una versione più grande del grafico, seleziona **Zoom vista**.

Viene visualizzato il grafico comparativo dei componenti del cluster. È possibile limitare il confronto deselegionando o selezionando l'opzione  associato a ciascun componente del cluster.

3. Per visualizzare i valori specifici, sposta il cursore nell'area del grafico per visualizzare la finestra popup.

Visualizza il traffico IOPS SVM per protocollo

È possibile visualizzare informazioni dettagliate sugli IOPS per una SVM utilizzando la pagina Performance/SVM Explorer. Il grafico del contatore IOPS - Totale mostra l'utilizzo totale degli IOPS sulla SVM, mentre il grafico del contatore IOPS - Suddivisione è utile per determinare l'impatto di lettura, scrittura e altri IOPS sulla SVM.

Inoltre, il grafico 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-FC

Passi

1. Nella pagina **Performance/SVM Explorer** per l'SVM selezionato, dal grafico IOPS, seleziona **Protocolli** dal menu a discesa.

Viene visualizzato il grafico IOPS - Protocolli.

2. Per visualizzare una versione più grande del grafico, seleziona **Zoom vista**.

Viene visualizzato il grafico comparativo del protocollo avanzato IOPS. È possibile limitare il confronto deselegionando o selezionando l'opzione  che è associato a un protocollo.

3. Per visualizzare i valori specifici, spostare il cursore nell'area del grafico per visualizzare la finestra popup.

Visualizza i grafici di volume e latenza LUN per verificare la garanzia delle prestazioni

È possibile visualizzare i volumi e i LUN a cui si è sottoscritto il programma “Performance Guarantee” per verificare che la latenza non abbia superato il livello garantito.

La garanzia di prestazioni di latenza è un valore di millisecondi per operazione che non deve essere superato. Si basa su una media oraria e non sul periodo predefinito di raccolta delle prestazioni di cinque minuti.

Passi

1. Nella vista **Prestazioni: Tutti i volumi** o nella vista **Prestazioni: Tutti i LUN**, seleziona il volume o il LUN che ti interessa.
2. Nella pagina **Performance Explorer** per il volume o LUN selezionato, seleziona **Media oraria** dal selettore **Visualizza statistiche in**.

La linea orizzontale nel grafico della latenza mostrerà una linea più uniforme man mano che le raccolte di cinque minuti vengono sostituite dalla media oraria.

3. Se sullo stesso aggregato sono presenti altri volumi coperti dalla garanzia sulle prestazioni, è possibile aggiungere tali volumi per visualizzarne il valore di latenza nello stesso grafico.

Visualizza le prestazioni per tutti i cluster SAN Array

È possibile utilizzare la vista **Prestazioni: Tutti i cluster** per visualizzare lo stato delle prestazioni di tutti i cluster SAN Array.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile visualizzare informazioni generali per tutti i cluster SAN Array nella vista **Prestazioni: Tutti i cluster** e dettagli nella pagina **Cluster/Esplora prestazioni**.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.
2. Assicurarsi che la colonna “Personalità” sia visualizzata nella vista **Salute: Tutti i cluster** oppure aggiungerla utilizzando il controllo **Mostra / Nascondi**.

Questa colonna visualizza “All SAN Array” per i cluster All SAN Array.

3. Per visualizzare informazioni sulle prestazioni in tali cluster, selezionare la vista **Prestazioni: tutti i cluster**.

Visualizza le informazioni sulle prestazioni per il cluster All SAN Array.

4. Per visualizzare informazioni dettagliate sulle prestazioni di tali cluster, fare clic sul nome di un cluster All SAN Array.
5. Fare clic sulla scheda **Esplora**.
6. Nella pagina **Cluster / Performance Explorer**, seleziona **Nodi su questo cluster** dal menu **Visualizza e confronta**.

È possibile confrontare le statistiche delle prestazioni di entrambi i nodi su questo cluster per assicurarsi che il carico sia pressoché identico su entrambi i nodi. Se ci sono grandi discrepanze tra i due nodi, puoi aggiungere il secondo nodo ai grafici e confrontare i valori su un intervallo di tempo più lungo per identificare eventuali problemi di configurazione.

Visualizza gli IOPS del nodo in base ai carichi di lavoro che risiedono solo sul nodo locale

Il grafico del contatore IOPS del nodo può evidenziare dove le operazioni passano solo attraverso il nodo locale utilizzando un LIF di rete per eseguire operazioni di lettura/scrittura su volumi su un nodo remoto. I grafici IOPS - “Totale (Locale)” e “Ripartizione (Locale)” mostrano gli IOPS per i dati che risiedono solo nei volumi locali sul nodo corrente.

Le versioni “Locali” di questi grafici dei contatori sono simili ai grafici dei nodi per Capacità e Utilizzo delle prestazioni, perché mostrano anche solo le statistiche per i dati che risiedono su volumi locali.

Confrontando le versioni “Locali” di questi grafici dei contatori con le normali versioni Total di questi grafici dei contatori, è possibile vedere se c’è molto traffico in transito attraverso il nodo locale per accedere ai volumi sul nodo remoto. Questa situazione potrebbe causare problemi di prestazioni, probabilmente indicati da un utilizzo elevato sul nodo, se ci sono troppe operazioni che passano attraverso il nodo locale per raggiungere un volume su un nodo remoto. In questi casi potrebbe essere necessario spostare un volume sul nodo locale oppure creare un LIF sul nodo remoto in cui è possibile connettere il traffico proveniente dagli host che accedono a tale volume.

Passi

1. Nella pagina **Prestazioni/Esplora nodi** del nodo selezionato, dal grafico IOPS, seleziona **Totale** dal menu a discesa.

Viene visualizzato il grafico IOPS - Totale.

2. Fare clic su **Zoom vista** per visualizzare una versione più grande del grafico in una nuova scheda del browser.
3. Tornando alla pagina **Prestazioni/Esplora nodi**, dal grafico IOPS, seleziona **Totale (Locale)** dal menu a discesa.

Viene visualizzato il grafico IOPS - Totale (Locale).

4. Fare clic su **Zoom vista** per visualizzare una versione più grande del grafico in una nuova scheda del browser.
5. Osserva entrambi i grafici uno accanto all’altro e individua le aree in cui i valori IOPS sembrano essere piuttosto diversi.
6. Sposta il cursore su queste aree per confrontare gli IOPS locali e totali per un momento specifico.

Componenti delle landing page degli oggetti

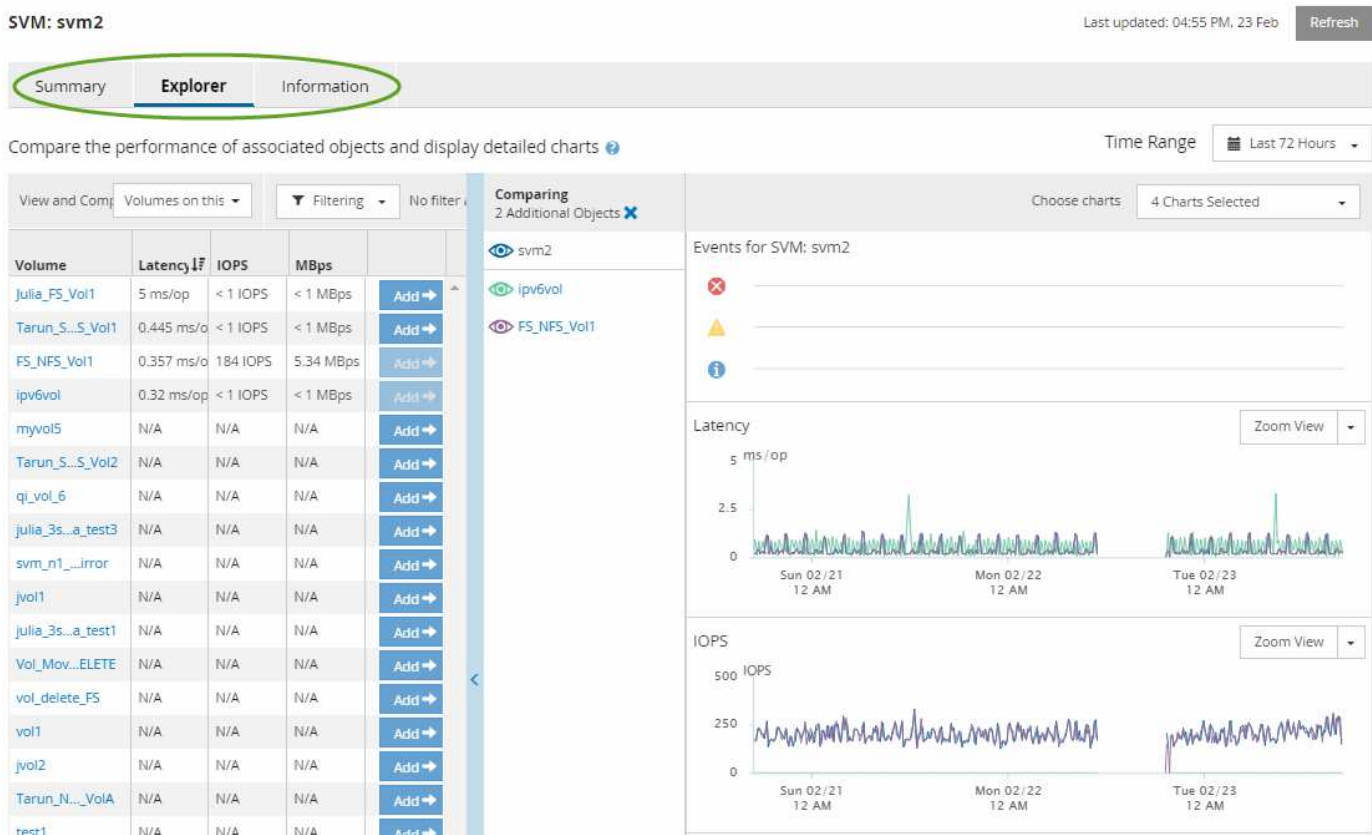
Le pagine di destinazione degli oggetti forniscono dettagli su tutti gli eventi critici, di avviso e informativi. Forniscono una visione dettagliata delle prestazioni di tutti gli oggetti del cluster, consentendo di selezionare e confrontare singoli oggetti in diversi periodi di tempo.

Le pagine di destinazione degli oggetti consentono di esaminare le prestazioni complessive di tutti gli oggetti e di confrontare i dati sulle prestazioni degli oggetti in un formato affiancato. Ciò è utile quando si valutano le prestazioni e si risolvono i problemi degli eventi.



I dati visualizzati nei pannelli riepilogativi dei contatori e nei grafici dei contatori si basano su un intervallo di campionamento di cinque minuti. I dati visualizzati nella griglia dell'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 una pagina di destinazione dell'oggetto che visualizza le informazioni di Explorer:



A seconda dell'oggetto di archiviazione visualizzato, la pagina di destinazione dell'oggetto può contenere le seguenti schede che forniscono dati sulle prestazioni dell'oggetto:

- Riepilogo**
Visualizza tre o quattro grafici contatori contenenti gli eventi e le prestazioni per oggetto per il periodo di 72 ore precedente, inclusa una linea di tendenza che mostra i valori massimi e minimi durante quel periodo.
- Esploratore**
Visualizza una griglia di oggetti di archiviazione correlati all'oggetto corrente, che consente di confrontare i valori delle prestazioni dell'oggetto corrente con quelli degli oggetti correlati. Questa scheda include fino a undici grafici contatori e un selettore di intervallo temporale, che consentono di effettuare una serie di confronti.
- Informazioni**
Visualizza i valori per gli attributi di configurazione non prestazionali relativi all'oggetto di archiviazione, tra

cui la versione installata del software ONTAP , il nome del partner HA e il numero di porte e LIF.

- **I migliori artisti**

Per i cluster: visualizza gli oggetti di archiviazione con le prestazioni più elevate o più basse, in base al contatore delle prestazioni selezionato.

- **Pianificazione del failover**

Per i nodi: visualizza la stima dell'impatto sulle prestazioni di un nodo in caso di guasto del partner HA del nodo.

- **Dettagli**

Per i volumi: visualizza statistiche dettagliate sulle prestazioni per tutte le attività e le operazioni di I/O per il carico di lavoro del volume selezionato. Questa scheda è disponibile per i volumi FlexVol , i volumi FlexGroup e i componenti dei FlexGroup.

Pagina di riepilogo

La pagina Riepilogo visualizza grafici dei contatori contenenti dettagli sugli eventi e sulle prestazioni per oggetto per il periodo di 72 ore precedente. Questi dati non vengono aggiornati automaticamente, ma sono aggiornati all'ultimo caricamento della pagina. I grafici nella pagina Riepilogo rispondono alla domanda *Devo cercare oltre?*

Grafici e statistiche del contatore

I grafici riepilogativi forniscono una rapida panoramica di alto livello per le ultime 72 ore e aiutano a identificare possibili problemi che richiedono ulteriori indagini.

Le statistiche del contatore della pagina Riepilogo vengono visualizzate nei grafici.

È possibile posizionare il cursore sulla linea di tendenza in un grafico per visualizzare i valori del contatore per un determinato momento. I grafici riepilogativi mostrano 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 di I/O; espresso in millisecondi per operazione.

Visualizzato per tutti i tipi di oggetto.

- **IOPS**

Velocità media di funzionamento; espressa in operazioni di input/output al secondo.

Visualizzato per tutti i tipi di oggetto.

- **MB/s**

Capacità di elaborazione media; espressa in megabyte al secondo.

Visualizzato per tutti i tipi di oggetto.

- **Capacità di prestazione utilizzata**

Percentuale della capacità di prestazione consumata da un nodo o da un aggregato.

Visualizzato solo per nodi e aggregati.

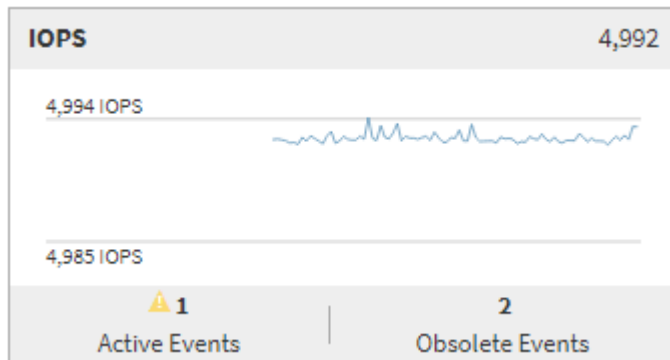
- **Utilizzo**

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 conteggio degli eventi per Eventi attivi vengono visualizzati il tipo e il numero di eventi. Gli eventi critici vengono visualizzati in rosso (■), e gli eventi di avviso vengono visualizzati in giallo (■).

Il numero in alto a destra del grafico, nella barra grigia, è il valore medio delle ultime 72 ore. I numeri mostrati nella parte inferiore e superiore del grafico della linea di tendenza rappresentano i valori minimo e massimo dell'ultimo periodo di 72 ore. La barra grigia sotto il grafico contiene il conteggio degli eventi attivi (nuovi e riconosciuti) e degli eventi obsoleti dell'ultimo periodo di 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 medio di risposta per tutte le richieste di I/O; espresso in millisecondi per operazione, al tempo di servizio, al tempo di attesa o ad entrambi sperimentati da un pacchetto di dati o da un blocco nel componente di archiviazione del cluster in esame.

In alto (valore del contatore): il numero nell'intestazione mostra la media del periodo di 72 ore precedente.

Centro (grafico delle prestazioni): il numero nella parte inferiore del grafico indica la latenza più bassa, mentre il numero nella parte superiore del grafico indica la latenza più alta per il periodo di 72 ore precedente. Posiziona il cursore sulla linea di tendenza del grafico per visualizzare il valore di latenza per un tempo specifico.

In basso (eventi): Passando il mouse sopra, il pop-up mostra 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 IOPS**

Il grafico del contatore IOPS fornisce una panoramica di alto livello dello stato IOPS dell'oggetto per il

periodo di 72 ore precedente. IOPS indica la velocità del sistema di archiviazione in numero di operazioni di input/output al secondo.

In alto (valore del contatore): il numero nell'intestazione mostra la media del periodo di 72 ore precedente.

Centro (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 alti per il periodo di 72 ore precedente. Posiziona il cursore sulla linea di tendenza del grafico per visualizzare il valore IOPS per un periodo di tempo specifico.

In basso (eventi): Passando il mouse sopra, il pop-up mostra 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 MB/s**

Il grafico del contatore MB/s mostra le prestazioni MB/s dell'oggetto e indica quanti dati sono stati trasferiti da e verso l'oggetto in megabyte al secondo. Il grafico del contatore MB/s fornisce una panoramica di alto livello dello stato di salute in MB/s dell'oggetto per il periodo di 72 ore precedente.

In alto (valore del contatore): il numero nell'intestazione mostra il numero medio di MB/s per il periodo di 72 ore precedente.

Centro (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. Posiziona il cursore sulla linea di tendenza del grafico per visualizzare il valore MB/s per un periodo di tempo specifico.

In basso (eventi): Passando il mouse sopra, il pop-up mostra 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.

- **Tabella del contatore della capacità prestazionale utilizzata**

Il grafico del contatore Capacità di prestazione utilizzata mostra la percentuale di capacità di prestazione utilizzata dall'oggetto.

In alto (valore del contatore): il numero nell'intestazione mostra la capacità di prestazione media utilizzata per il periodo di 72 ore precedente.

Centro (grafico delle prestazioni): il valore nella parte inferiore del grafico mostra la percentuale di capacità di prestazioni utilizzata più bassa, mentre il valore nella parte superiore del grafico mostra la percentuale di capacità di prestazioni utilizzata più alta per il periodo di 72 ore precedente. Posiziona il cursore sulla linea di tendenza del grafico per visualizzare il valore della capacità prestazionale utilizzata per un periodo di tempo specifico.

In basso (eventi): Passando il mouse sopra, il pop-up mostra 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 mostra la percentuale di utilizzo dell'oggetto. 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.

In alto (valore del contatore): il numero nell'intestazione mostra la percentuale media di utilizzo per il periodo di 72 ore precedente.

Centro (grafico delle prestazioni): il valore nella parte inferiore del grafico mostra la percentuale di utilizzo più bassa, mentre il valore nella parte superiore del grafico mostra la percentuale di utilizzo più alta per il periodo di 72 ore precedente. Posiziona il cursore sulla linea di tendenza del grafico per visualizzare il valore di utilizzo per un periodo di tempo specifico.

In basso (eventi): Passando il mouse sopra, il pop-up mostra 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, ove applicabile, elenca gli eventi più recenti che si sono verificati su quell'oggetto. Facendo clic sul nome dell'evento vengono visualizzati i dettagli dell'evento nella pagina Dettagli evento.

Componenti della pagina Performance Explorer

La pagina Performance Explorer consente di confrontare le prestazioni di oggetti simili in un cluster, ad esempio tutti i volumi in un cluster. Ciò è utile quando si risolvono problemi relativi alle prestazioni e si ottimizzano le prestazioni degli oggetti. È anche possibile confrontare gli oggetti con l'oggetto radice, che rappresenta la base di riferimento rispetto alla quale vengono effettuati altri confronti tra oggetti.

È possibile fare clic sul pulsante **Passa alla visualizzazione Salute** per visualizzare la pagina dei dettagli Salute per questo oggetto. In alcuni casi è possibile ottenere informazioni importanti sulle impostazioni di configurazione dell'archiviazione per questo oggetto, che potrebbero rivelarsi utili per la risoluzione di un problema.

La pagina Performance Explorer visualizza un elenco di oggetti cluster e i relativi dati sulle prestazioni. Questa pagina visualizza tutti gli oggetti del cluster dello stesso tipo (ad esempio, volumi e statistiche sulle prestazioni specifiche dell'oggetto) in formato tabellare. Questa vista fornisce una panoramica efficiente delle prestazioni degli oggetti cluster.



Se in una cella della tabella compare "N/D", significa che un valore per quel contatore non è disponibile perché in quel momento non c'è 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 oppure 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 radice e dai dati disponibili. È possibile fare clic sull'elenco a discesa Visualizza e confronta per selezionare un tipo di oggetto. Il tipo di oggetto selezionato

viene visualizzato nell'elenco.

- **Filtro**

Ti consente di restringere la quantità di dati che ricevi, in base alle tue preferenze.

È possibile creare filtri da applicare ai dati dell'oggetto, ad esempio IOPS maggiori di 4. È possibile aggiungere fino a quattro filtri contemporaneamente.

- **Confronto**

Visualizza un elenco degli oggetti selezionati per il confronto con l'oggetto radice.

I dati degli oggetti nel riquadro Confronto vengono visualizzati nei grafici Contatore.

- **Visualizza le statistiche in**

Per volume e LUN, consente di selezionare se le statistiche vengono visualizzate dopo ogni ciclo di raccolta (impostazione predefinita: 5 minuti) oppure se vengono mostrate come media oraria. Questa funzionalità consente di visualizzare il grafico della latenza a supporto del programma NetApp "Performance Guarantee".

- **Grafici di contropartita**

Visualizza i dati rappresentati graficamente per ogni categoria di prestazioni dell'oggetto.

Di solito, 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 degli eventi**

Visualizza gli eventi relativi a prestazioni e stato di salute che si verificano nella sequenza temporale selezionata nel componente Intervallo di tempo.

Gestire le prestazioni 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 tramite il software ONTAP (System Manager o ONTAP CLI) o tramite le policy Unified Manager Performance Service Level. Unified Manager visualizza anche quali volumi e LUN hanno un gruppo di policy QoS assegnato.

Per ulteriori informazioni sulla regolazione delle impostazioni QoS, vedere ["Panoramica sulla gestione delle prestazioni"](#)

Come la qualità del servizio di archiviazione può controllare la produttività del carico di lavoro

È possibile creare un gruppo di policy di qualità del servizio (QoS) per controllare il limite di I/O al secondo (IOPS) o di 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 proprie esigenze, è possibile aumentare il limite o spostare i carichi di lavoro in un gruppo di policy nuovo o esistente che abbia il limite desiderato.

I gruppi di policy QoS "tradizionali" possono essere assegnati a singoli carichi di lavoro, ad esempio a un singolo volume o LUN. In questo caso il carico di lavoro può utilizzare il limite di throughput completo. I gruppi di policy QoS possono anche essere assegnati a più carichi di lavoro; in tal caso il limite di throughput viene "condiviso" tra i carichi di lavoro. Ad esempio, un limite QoS di 9.000 IOPS assegnato a tre carichi di lavoro impedirebbe che gli IOPS combinati superino i 9.000 IOPS.

I gruppi di policy QoS "Adaptive" possono essere assegnati anche a carichi di lavoro singoli o a più carichi di lavoro. Tuttavia, anche quando assegnato a più carichi di lavoro, ogni carico di lavoro ottiene il limite di throughput completo anziché condividere il valore di throughput con altri carichi di lavoro. Inoltre, i criteri QoS adattivi regolano automaticamente l'impostazione della velocità effettiva in base alle dimensioni del volume, per 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 una velocità massima di elaborazione di 50.000 IOPS. Se il volume viene successivamente ridimensionato a 20 TB, la QoS adattiva regola il massimo a 100.000 IOPS.

A partire da ONTAP 9.5 è possibile includere la dimensione del blocco quando si definisce una policy QoS adattiva. In questo modo, la policy viene convertita da una soglia IOPS/TB a una soglia MB/s nei casi in cui i carichi di lavoro utilizzano blocchi di dimensioni molto grandi e, in definitiva, una percentuale elevata di throughput.

Per le policy QoS di gruppo condivise, quando gli IOPS o gli MB/s di tutti i carichi di lavoro in un gruppo di policy superano il limite impostato, il gruppo di policy limita i carichi di lavoro per limitarne l'attività, il che può ridurre le prestazioni di tutti i carichi di lavoro nel gruppo di policy. Se un evento di prestazioni dinamiche viene generato dalla limitazione del gruppo di policy, la descrizione dell'evento visualizza il nome del gruppo di policy coinvolto.

Nella vista Prestazioni: tutti i volumi, è possibile ordinare i volumi interessati in base a IOPS e MB/s per vedere quali carichi di lavoro hanno l'utilizzo più elevato che potrebbe aver contribuito all'evento. Nella pagina Performance/Volumes Explorer è possibile selezionare altri volumi o LUN sul volume per confrontarli con l'utilizzo di IOPS o MBps del carico di lavoro interessato.

Assegnando i carichi di lavoro che stanno utilizzando eccessivamente le risorse del nodo a un'impostazione di gruppo di policy più restrittiva, il gruppo di policy limita i carichi di lavoro per limitarne l'attività, il che può ridurre l'utilizzo delle risorse su quel nodo. Tuttavia, se si desidera che il carico di lavoro possa utilizzare più risorse del nodo, è possibile aumentare il valore del gruppo di policy.

È possibile utilizzare System Manager, i comandi ONTAP o Unified Manager Performance Service Levels per gestire i gruppi di policy, incluse le seguenti attività:

- Creazione di un gruppo di policy
- Aggiunta o rimozione di carichi di lavoro in un gruppo di policy
- Spostamento di un carico di lavoro tra gruppi di policy
- Modifica del limite di throughput di un gruppo di policy
- Spostamento di un carico di lavoro su un aggregato e/o nodo diverso

Visualizza tutti i gruppi di policy QoS disponibili su tutti i cluster

È possibile visualizzare un elenco di tutti i gruppi di policy QoS disponibili sui cluster monitorati da Unified Manager. Ciò include le policy QoS tradizionali, le policy QoS adattive e le policy QoS gestite dalle policy Unified Manager Performance Service Level.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Gruppi di criteri QoS**.

Per impostazione predefinita viene visualizzata la vista Prestazioni: Gruppi di criteri QoS tradizionali.

2. Visualizza le impostazioni di configurazione dettagliate per ciascun gruppo di policy QoS tradizionali disponibili.
3. Fare clic sul pulsante Espandi () accanto al nome del gruppo di policy QoS per visualizzare maggiori dettagli sul gruppo di policy.
4. Nel menu Visualizza, seleziona una delle opzioni aggiuntive per visualizzare tutti i gruppi di policy QoS adattivi o per visualizzare tutti i gruppi di policy QoS creati utilizzando Unified Manager Performance Service Levels.

Visualizza volumi o LUN che si trovano nello stesso gruppo di policy QoS

È possibile visualizzare un elenco dei volumi e dei LUN assegnati allo stesso gruppo di policy QoS.

Nel caso di gruppi di policy QoS tradizionali “condivisi” tra più volumi, questo può essere utile per verificare se determinati volumi stanno sovrautilizzando la velocità effettiva definita per il gruppo di policy. Può anche aiutarti a decidere se puoi aggiungere altri volumi al gruppo di policy senza che ciò abbia un effetto negativo sugli altri volumi.

Nel caso di policy QoS adattive e policy Unified Manager Performance Service Levels, può essere utile visualizzare tutti i volumi o LUN che utilizzano un gruppo di policy, in modo da poter vedere quali oggetti sarebbero interessati se si modificassero le impostazioni di configurazione per la policy QoS.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Gruppi di criteri QoS**.

Per impostazione predefinita viene visualizzata la vista Prestazioni: Gruppi di criteri QoS tradizionali.

2. Se sei interessato ai gruppi di politica tradizionale, resta su questa pagina. In caso contrario, selezionare una delle opzioni di visualizzazione aggiuntive per visualizzare tutti i gruppi di policy QoS adattivi o tutti i gruppi di policy QoS creati da Unified Manager Performance Service Levels.
3. Nella policy QoS che ti interessa, clicca sul pulsante Espandi () accanto al nome del gruppo di criteri QoS per visualizzare maggiori dettagli.

View Adaptive QoS Policy Groups Search Quality of Service

QoS Policy Group	Cluster	SVM	Min Through...	Max Through...	Absolute Min...	Block Size	Asso
▼ julia_vs2_cifs_Performance	opm-simplicity	julia_vs2_cifs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		1
▲ julia_vs1_nfs_Performance	opm-simplicity	julia_vs1_nfs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		2
Details Allocated Capacity 0.99 TB 1.15 TB Associated Objects 2 Volumes 0 LUNs Events None							
▼ julia_nfs_extreme_Extreme_Performance	ocum-mobility-01-02	julia_nfs_extreme	6144.0 IOPS/TB	12288.0 IOPS/TB	1000IOPS	any	1
▼ julia_extreme_jan16_aqos	ocum-mobility-01-02	julia_nfs_extreme	10000.0 IOPS/TB	12000.0 IOPS/TB	1000IOPS	any	1

4. Fare clic sul collegamento Volumi o LUN per visualizzare gli oggetti che utilizzano questo criterio QoS.

Viene visualizzata la pagina Inventario prestazioni per volumi o LUN con l'elenco ordinato degli oggetti che utilizzano il criterio QoS.

Visualizza le impostazioni del gruppo di criteri QoS applicate a volumi o LUN specifici

È possibile visualizzare i gruppi di policy QoS applicati ai volumi e alle LUN ed è possibile collegarsi alla vista Gruppi di policy QoS/Prestazioni per visualizzare le impostazioni di configurazione dettagliate per ciascuna policy QoS.

Di seguito sono riportati i passaggi per visualizzare la policy QoS applicata a un volume. I passaggi per visualizzare queste informazioni per una LUN sono simili.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.

Per impostazione predefinita viene visualizzata la vista Integrità: Tutti i volumi.

2. Nel menu Visualizza, selezionare **Prestazioni: Volumi nel gruppo di criteri QoS**.
3. Individua il volume che desideri esaminare e scorri verso destra finché non vedi la colonna **Gruppo criteri QoS**.
4. Fare clic sul nome del gruppo di criteri QoS.

La pagina Qualità del servizio corrispondente viene visualizzata a seconda che si tratti di un criterio QoS tradizionale, di un criterio QoS adattivo o di un criterio QoS creato utilizzando Unified Manager Performance Service Levels.

5. Visualizza le impostazioni di configurazione dettagliate per il gruppo di policy QoS.
6. Fare clic sul pulsante Espandi (▼) accanto al nome del gruppo di policy QoS per visualizzare maggiori dettagli sul gruppo di policy.

Visualizza i grafici delle prestazioni per confrontare volumi o LUN che si trovano nello stesso gruppo di policy QoS

È possibile visualizzare i volumi e i LUN che si trovano negli stessi gruppi di policy QoS e quindi confrontare le prestazioni 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 policy QoS. I passaggi per visualizzare queste informazioni per una LUN sono simili.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.

Per impostazione predefinita viene visualizzata la vista Integrità: Tutti i volumi.

2. Nel menu Visualizza, selezionare **Prestazioni: Volumi nel gruppo di criteri QoS**.
3. Fare clic sul nome del volume che si desidera esaminare.

Viene visualizzata la pagina Performance Explorer per il volume.

4. Nel menu Visualizza e confronta, seleziona **Volumi nello stesso gruppo di criteri QoS**.

Gli altri volumi che condividono la stessa politica QoS sono elencati nella tabella seguente.

5. Fare clic sul pulsante **Aggiungi** per aggiungere tali 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 in intervalli di tempo diversi da quello predefinito 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) definiti da ONTAP che sono stati applicati a un volume o a una 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 criterio QoS applicato al carico di lavoro.

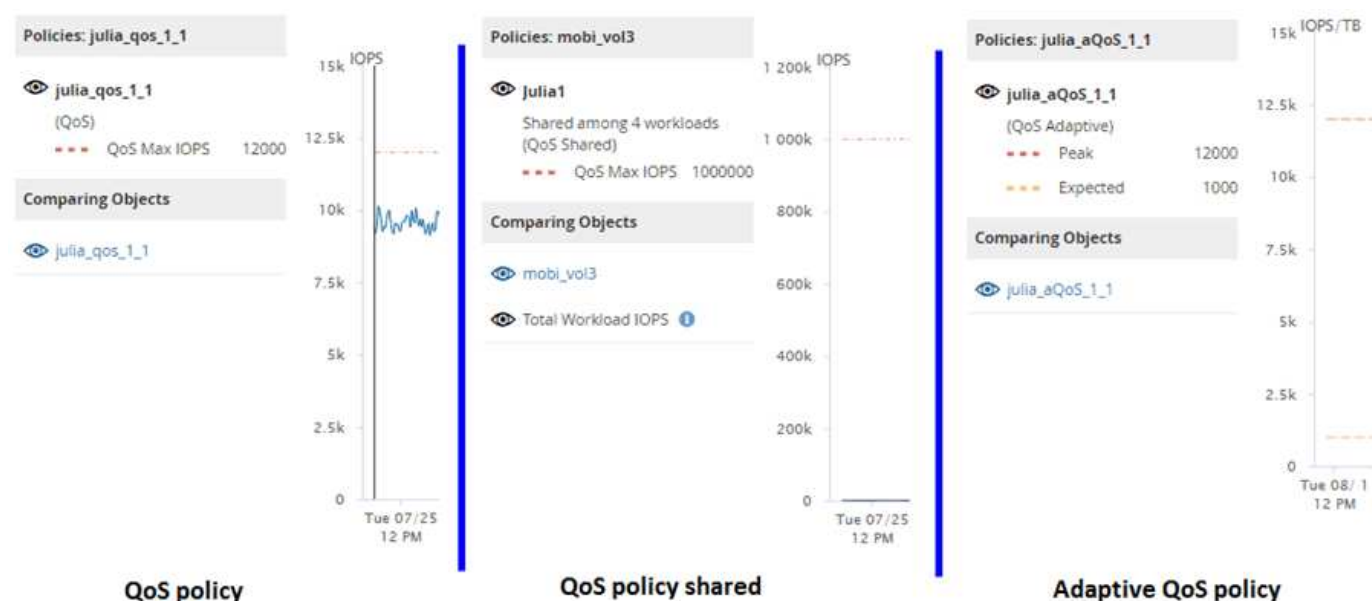
Un'impostazione di throughput massimo (o "picco") definisce il throughput massimo che il carico di lavoro può consumare e limita quindi l'impatto sui carichi di lavoro concorrenti per le risorse di sistema. Un'impostazione di throughput minimo (o "previsto") definisce il throughput minimo che deve essere disponibile per il carico di lavoro affinché un carico di lavoro critico soddisfi gli obiettivi di throughput minimo indipendentemente dalla domanda dei carichi di lavoro concorrenti.

Le policy QoS condivise e non condivise per IOPS e MB/s utilizzano i termini "minimo" e "massimo" per definire il limite minimo e massimo. Le policy QoS adattive per IOPS/TB, introdotte in ONTAP 9.3, utilizzano i termini "previsto" e "picco" per definire il limite minimo e massimo.

Sebbene ONTAP consenta di creare questi due tipi di policy QoS, a seconda di come vengono applicate ai carichi di lavoro, esistono tre modi in cui la policy QoS verrà visualizzata nei grafici delle prestazioni.

Tipo di politica	Funzionalità	Indicatore nell'interfaccia di Unified Manager
Criterio QoS condiviso assegnato a un singolo carico di lavoro o criterio QoS non condiviso assegnato a un singolo carico di lavoro o a più carichi di lavoro	Ogni carico di lavoro può consumare l'impostazione di throughput specificata	Visualizza "(QoS)"
Criterio QoS condiviso assegnato a più carichi di lavoro	Tutti i carichi di lavoro condividono l'impostazione di throughput specificata	Visualizza "(QoS condiviso)"
Criterio QoS adattivo assegnato a un singolo carico di lavoro o a più carichi di lavoro	Ogni carico di lavoro può consumare l'impostazione di throughput specificata	Visualizza "(QoS adattivo)"

La figura seguente mostra un esempio di come vengono rappresentate le tre opzioni nei grafici dei contatori.



Quando una normale policy QoS definita in IOPS appare nel grafico IOPS/TB per un carico di lavoro, ONTAP converte il valore IOPS in un valore IOPS/TB e Unified Manager visualizza tale policy nel grafico IOPS/TB insieme al testo "QoS, definito in IOPS".

Quando un criterio QoS adattivo definito in IOPS/TB appare nel grafico IOPS per un carico di lavoro, ONTAP converte il valore IOPS/TB in un valore IOPS e Unified Manager visualizza tale criterio nel grafico IOPS insieme al testo "QoS adattivo - Utilizzato, definito in IOPS/TB" o "QoS adattivo - Allocato, definito 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", il picco di IOPS viene calcolato in base alle dimensioni del volume. Quando l'impostazione di allocazione è impostata su "used-space", il picco IOPS viene calcolato in base alla quantità di dati archiviati nel volume, tenendo conto dell'efficienza di archiviazione.



Il grafico IOPS/TB visualizza i dati sulle prestazioni solo quando la capacità logica utilizzata dal volume è maggiore o uguale a 128 GB. Nel grafico vengono visualizzati degli spazi vuoti quando la capacità utilizzata scende al di sotto di 128 GB durante l'intervallo di tempo selezionato.

Visualizza le impostazioni minime e massime della qualità del servizio del carico di lavoro in Performance Explorer

È possibile visualizzare le impostazioni dei criteri di qualità del servizio (QoS) definiti da ONTAP su un volume o LUN nei grafici di Performance Explorer. Un'impostazione di throughput massimo limita l'impatto dei carichi di lavoro concorrenti sulle risorse di sistema. Un'impostazione minima di throughput garantisce che un carico di lavoro critico soddisfi gli obiettivi minimi di throughput indipendentemente dalla domanda dei carichi di lavoro concorrenti.

Le impostazioni "minimo" e "massimo" della velocità di trasmissione QoS, IOPS e MB/s vengono visualizzate nei grafici dei contatori solo se sono state configurate in ONTAP. Le impostazioni minime di throughput sono disponibili solo sui sistemi che eseguono il software ONTAP 9.2 o versioni successive, solo sui sistemi AFF e al momento possono essere impostate solo per IOPS.

Le policy QoS adattive sono disponibili a partire da ONTAP 9.3 e vengono espresse utilizzando IOPS/TB anziché IOPS. Queste policy regolano automaticamente il valore della policy QoS in base alle dimensioni del volume, per carico di lavoro, mantenendo così il rapporto tra IOPS e terabyte al variare delle dimensioni del volume. È possibile applicare un gruppo di policy QoS adattivo solo ai volumi. Per le policy QoS adattive vengono utilizzati i termini "previsto" e "picco" anziché minimo e massimo.

Unified Manager genera eventi di avviso per violazioni dei criteri QoS quando la velocità effettiva del carico di lavoro ha superato l'impostazione massima dei criteri QoS definita durante ogni periodo di raccolta delle prestazioni per l'ora precedente. La produttività del carico di lavoro potrebbe superare la soglia QoS solo per un breve periodo di tempo durante ogni periodo di raccolta, ma Unified Manager visualizza la produttività "media" durante il periodo di raccolta nel grafico. Per questo motivo potrebbero essere visualizzati eventi QoS anche se la velocità effettiva di un carico di lavoro potrebbe non aver superato la soglia della policy indicata nel grafico.

Passi

1. Nella pagina **Performance Explorer** per il volume o LUN selezionato, eseguire le seguenti azioni per visualizzare le impostazioni del limite massimo e minimo di QoS:

Se lo desidera...	Fai questo...
Visualizza il limite massimo di IOPS (QoS massimo)	Nel grafico IOPS totale o ripartizione, fare clic su Zoom vista .
Visualizza il limite MB/s (QoS max)	Nel grafico MB/s Totale o Ripartizione, fare clic su Vista Zoom .
Visualizza il pavimento IOPS (il minimo QoS)	Nel grafico IOPS totale o ripartizione, fare clic su Zoom vista .

Se lo desidera...	Fai questo...
Visualizza il limite massimo di IOPS/TB (il picco QoS)	Per i volumi, nel grafico IOPS/TB, fare clic su Zoom vista .
Visualizza il livello minimo IOPS/TB (la QoS prevista)	Per i volumi, nel grafico IOPS/TB, fare clic su Zoom vista .

La linea orizzontale tratteggiata indica il valore massimo o minimo di throughput impostato in ONTAP. È anche possibile visualizzare quando sono state implementate le modifiche ai valori QoS.

2. Per visualizzare i valori specifici di IOPS e MB/s confrontati con l'impostazione QoS, spostare il cursore nell'area del grafico per visualizzare la finestra popup.

Se si nota che determinati volumi o LUN hanno IOPS o MB/s molto elevati e stanno sovraccaricando le risorse di sistema, è possibile utilizzare System Manager o ONTAP CLI per regolare le impostazioni 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 prestazioni"](#)

Gestire le prestazioni utilizzando la capacità delle prestazioni e le informazioni IOPS disponibili

La *capacità prestazionale* indica quanta produttività è possibile ottenere da una risorsa senza superare le prestazioni utili di tale risorsa. Se considerata utilizzando i contatori delle prestazioni esistenti, la capacità delle prestazioni è il punto in cui si ottiene il massimo utilizzo da un nodo o da un aggregato prima che la latenza diventi un problema.

Unified Manager raccoglie statistiche sulla capacità delle prestazioni dai nodi e le aggrega in ciascun cluster. La *capacità prestazionale utilizzata* è la percentuale di capacità prestazionale attualmente utilizzata, mentre la *capacità prestazionale libera* è la percentuale di capacità prestazionale ancora disponibile.

Mentre la capacità di prestazioni 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 prestazioni massima. Utilizzando questa metrica, puoi essere certo di poter aggiungere carichi di lavoro di un numero predeterminato di IOPS a una risorsa.

Monitorare le informazioni sulla capacità delle prestazioni presenta i seguenti vantaggi:

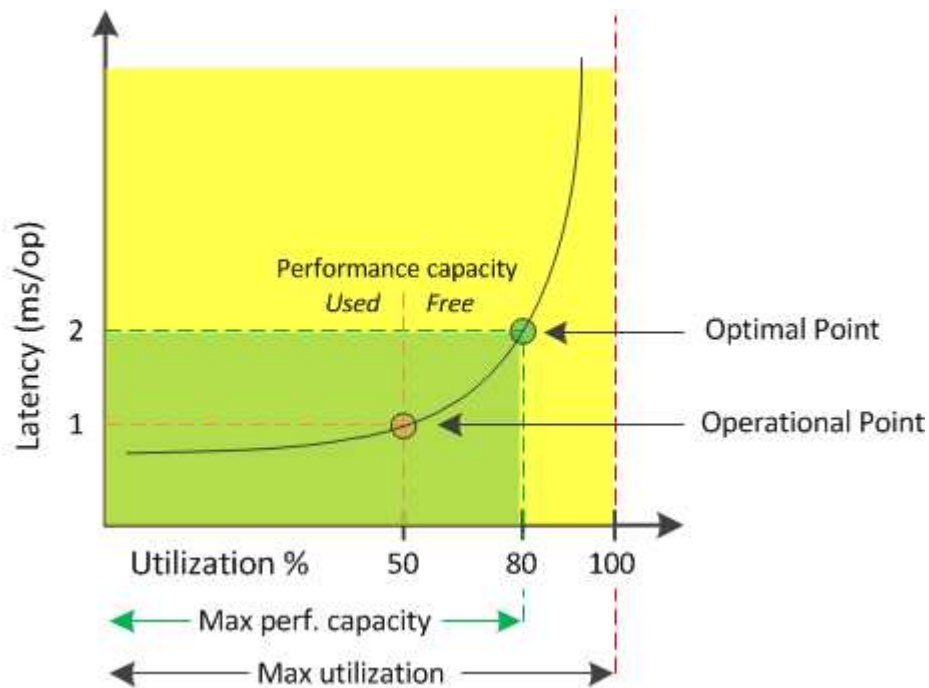
- Aiuta a predisporre e bilanciare il flusso di lavoro.
- Aiuta a prevenire il sovraccarico di un nodo o lo spostamento delle sue risorse oltre il punto ottimale, riducendo così la necessità di risolvere i problemi.
- Ti aiuta a determinare con maggiore precisione dove potrebbero essere necessarie attrezzature di stoccaggio aggiuntive.

Quale capacità di prestazione è utilizzata

Il contatore della capacità prestazionale utilizzata consente di identificare se le prestazioni di un nodo o di un aggregato stanno raggiungendo un punto in cui potrebbero

peggiore se i carichi di lavoro aumentano. Può anche mostrarti se un nodo o un aggregato è attualmente sovrautilizzato in determinati periodi di tempo. La capacità prestazionale utilizzata è simile all'utilizzo, ma la prima fornisce maggiori informazioni sulle capacità prestazionali disponibili in una risorsa fisica per un carico di lavoro specifico.

La capacità di prestazione ottimale utilizzata è il punto in cui un nodo o un aggregato ha un utilizzo e una latenza (tempo di risposta) ottimali e viene utilizzato in modo efficiente. Nella figura seguente è mostrata una curva di latenza rispetto all'utilizzo di un aggregato.



In questo esempio, il *punto operativo* identifica che l'aggregato sta attualmente operando al 50% di utilizzo con una latenza di 1,0 ms/op. Sulla base delle statistiche acquisite dall'aggregato, Unified Manager determina che per questo aggregato è disponibile ulteriore capacità di prestazioni. In questo esempio, il *punto ottimale* è identificato come il punto in cui l'aggregato è all'80% di utilizzo con una 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 prestazione utilizzata sia un numero maggiore rispetto al contatore "utilizzo" perché la capacità di prestazione aggiunge un impatto sulla latenza. Ad esempio, se un nodo o un aggregato viene utilizzato al 70%, il valore della capacità prestazionale potrebbe essere compreso tra l'80% e il 100%, a seconda del valore di latenza.

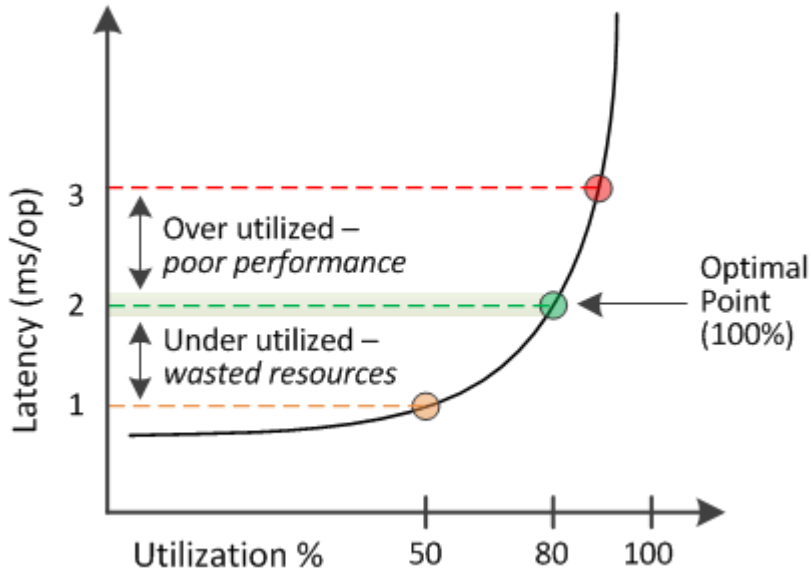
In alcuni casi, tuttavia, il contatore di utilizzo potrebbe essere più alto nella pagina Dashboard. Ciò è normale perché la dashboard aggiorna i valori correnti del contatore a ogni periodo di raccolta; non visualizza le medie su un periodo di tempo come le altre pagine nell'interfaccia utente di Unified Manager. Il contatore della capacità prestazionale utilizzata è più indicato come indicatore della prestazione media in un periodo di tempo, mentre il contatore di utilizzo è più indicato per determinare l'utilizzo istantaneo di una risorsa.

Cosa significa il valore della capacità prestazionale utilizzata

Il valore della capacità prestazionale utilizzata consente di identificare i nodi e gli aggregati che sono attualmente sovrautilizzati o sottoutilizzati. Ciò consente di

ridistribuire i carichi di lavoro per rendere più efficienti le risorse di archiviazione.

La figura seguente mostra la curva di latenza rispetto all'utilizzo di una risorsa e identifica, con punti colorati, tre aree in cui potrebbe essere localizzato il punto operativo corrente.



- Una percentuale di capacità prestazionale utilizzata pari al 100% è il punto ottimale.

In questo momento le risorse vengono utilizzate in modo efficiente.

- Una percentuale di capacità di prestazione utilizzata superiore a 100 indica che il nodo o l'aggregato è sovrutilizzato e che i carichi di lavoro stanno ricevendo prestazioni non ottimali.

Non è necessario aggiungere nuovi carichi di lavoro alla risorsa e potrebbe essere necessario ridistribuire i carichi di lavoro esistenti.

- Una percentuale di capacità di prestazione 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 altri carichi di lavoro alla risorsa.



A differenza dell'utilizzo, la percentuale di capacità prestazionale utilizzata può essere superiore al 100%. Non esiste una percentuale massima, ma in genere le risorse si aggirano tra il 110% e il 140% quando vengono sovrutilizzate. Percentuali più elevate indicherebbero una risorsa con problemi seri.

Quali IOPS sono disponibili

Il contatore IOPS disponibili identifica il numero rimanente di IOPS che possono essere aggiunti a un nodo o a un aggregato prima che la risorsa raggiunga il suo limite.

Il numero totale di IOPS che un nodo può fornire si basa sulle caratteristiche fisiche del nodo, ad esempio il numero di CPU, la velocità della CPU e la quantità di RAM. Il numero totale di IOPS che un aggregato può fornire si basa sulle proprietà fisiche dei dischi, ad esempio un disco SATA, SAS o SSD.

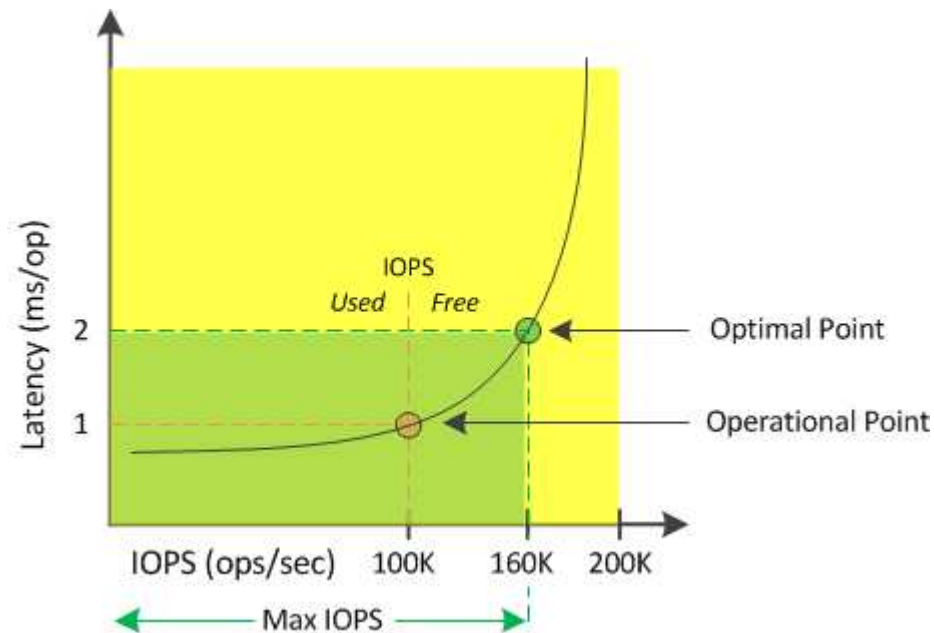
Il totale degli IOPS di tutti i volumi in un aggregato potrebbe non corrispondere al totale degli IOPS dell'aggregato. Questo argomento è trattato nel seguente articolo della knowledge base: KB"[Perché la somma](#)

di tutti gli IOP di volume in un aggregato non corrisponde agli IOP aggregati?"

Mentre il contatore della capacità di prestazioni disponibile fornisce la percentuale di una risorsa ancora disponibile, il contatore degli IOPS disponibili indica il numero esatto di IOPS (carichi di lavoro) che possono essere aggiunti a una risorsa prima di raggiungere la capacità di prestazioni massima.

Ad esempio, se si utilizzano una coppia di sistemi di archiviazione FAS2520 e FAS8060, un valore di capacità di prestazioni libera del 30% significa che si dispone di una certa capacità di prestazioni libera. Tuttavia, tale valore non fornisce visibilità su quanti altri carichi di lavoro è possibile distribuire su tali nodi. Il contatore IOPS disponibili potrebbe indicare che sono disponibili 500 IOPS sul FAS8060, ma solo 100 IOPS sul FAS2520.

Nella figura seguente è mostrato un esempio di curva di latenza rispetto a 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 prestazioni utilizzata è al 100% (punto ottimale). Il punto operativo identifica che il nodo sta attualmente operando a 100K IOPS con una 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 accade perché Unified Manager non dispone dei dati necessari per stimare con precisione le caratteristiche del carico di lavoro gestito.

Visualizza i valori utilizzati per la capacità di prestazione aggregata e del nodo

È possibile monitorare i valori della capacità prestazionale utilizzata per tutti i nodi o per tutti gli aggregati in un cluster, oppure è possibile visualizzare i dettagli per un singolo nodo o aggregato.

I valori della capacità prestazionale utilizzata vengono visualizzati nella Dashboard, nelle pagine Inventario prestazioni, nella pagina Migliori prestazioni, nella pagina Crea criterio soglia, nelle pagine Esplora prestazioni e nei grafici dettagliati. Ad esempio, la pagina Prestazioni: tutti gli aggregati fornisce una colonna Capacità di

prestazione utilizzata per visualizzare il valore della capacità di prestazione utilizzata per tutti gli aggregati.

Aggregates ⓘ

Last updated: 04:11 PM, 08 FebRefresh

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

FilteringNo filter applied

Search Aggregates DataSearch

Assign Threshold PolicyClear Threshold Policy

	Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
☐	✓	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
☐	✓	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
☐	✓	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
☐	✓	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
☐	✓	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
☐	✓	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
☐	✓	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
☐	✓	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS
☐	⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS

Monitorare il contatore della capacità prestazionale utilizzata consente di identificare quanto segue:

- Se i nodi o gli aggregati su qualsiasi cluster hanno un valore di capacità di prestazioni elevato utilizzato
- Se i nodi o gli aggregati su qualsiasi cluster hanno eventi di capacità di prestazioni attive utilizzati
- I nodi e gli aggregati che hanno la capacità di prestazioni più alta e più bassa vengono utilizzati in un cluster
- Valori del contatore di latenza e utilizzo in combinazione con nodi o aggregati che hanno valori di capacità di prestazioni elevate utilizzati
- In che modo i valori di capacità prestazionale utilizzati per i nodi in una coppia HA saranno influenzati se uno dei nodi fallisce
- I volumi e i LUN più occupati su un aggregato che ha un valore di capacità di prestazioni elevato utilizzato

Visualizza i nodi e aggrega i valori IOPS disponibili

È possibile monitorare i valori IOPS disponibili per tutti i nodi o per tutti gli aggregati in un cluster, oppure è possibile visualizzare i dettagli per un singolo nodo o aggregato.

I valori IOPS disponibili vengono visualizzati nelle pagine Inventario prestazioni e nei grafici delle pagine Esplora prestazioni per nodi e aggregati. Ad esempio, quando si visualizza un nodo nella pagina Node/Performance Explorer, è possibile selezionare il grafico del contatore "IOPS disponibili" dall'elenco, in modo da poter confrontare i valori IOPS disponibili per il nodo e più aggregati su quel nodo.



Monitorare il contatore IOPS disponibili consente di identificare:

- I nodi o gli aggregati che hanno i valori IOPS più elevati disponibili per aiutare a determinare dove potranno essere distribuiti 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 prestazioni futuri.
- I volumi e i LUN più occupati su un aggregato che ha un valore IOPS disponibile ridotto.

Visualizza i grafici del contatore della capacità di prestazione per identificare i problemi

È possibile visualizzare i grafici della capacità prestazionale utilizzata per nodi e aggregati nella pagina Performance Explorer. Ciò consente di visualizzare dati dettagliati sulla capacità delle prestazioni per i nodi e gli aggregati selezionati per un intervallo di tempo specifico.

Il grafico del contatore standard visualizza i valori della capacità prestazionale utilizzata per i nodi o gli aggregati selezionati. Il grafico del contatore di ripartizione mostra i valori totali della capacità di prestazione per l'oggetto radice, suddivisi 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 prestazione libera.

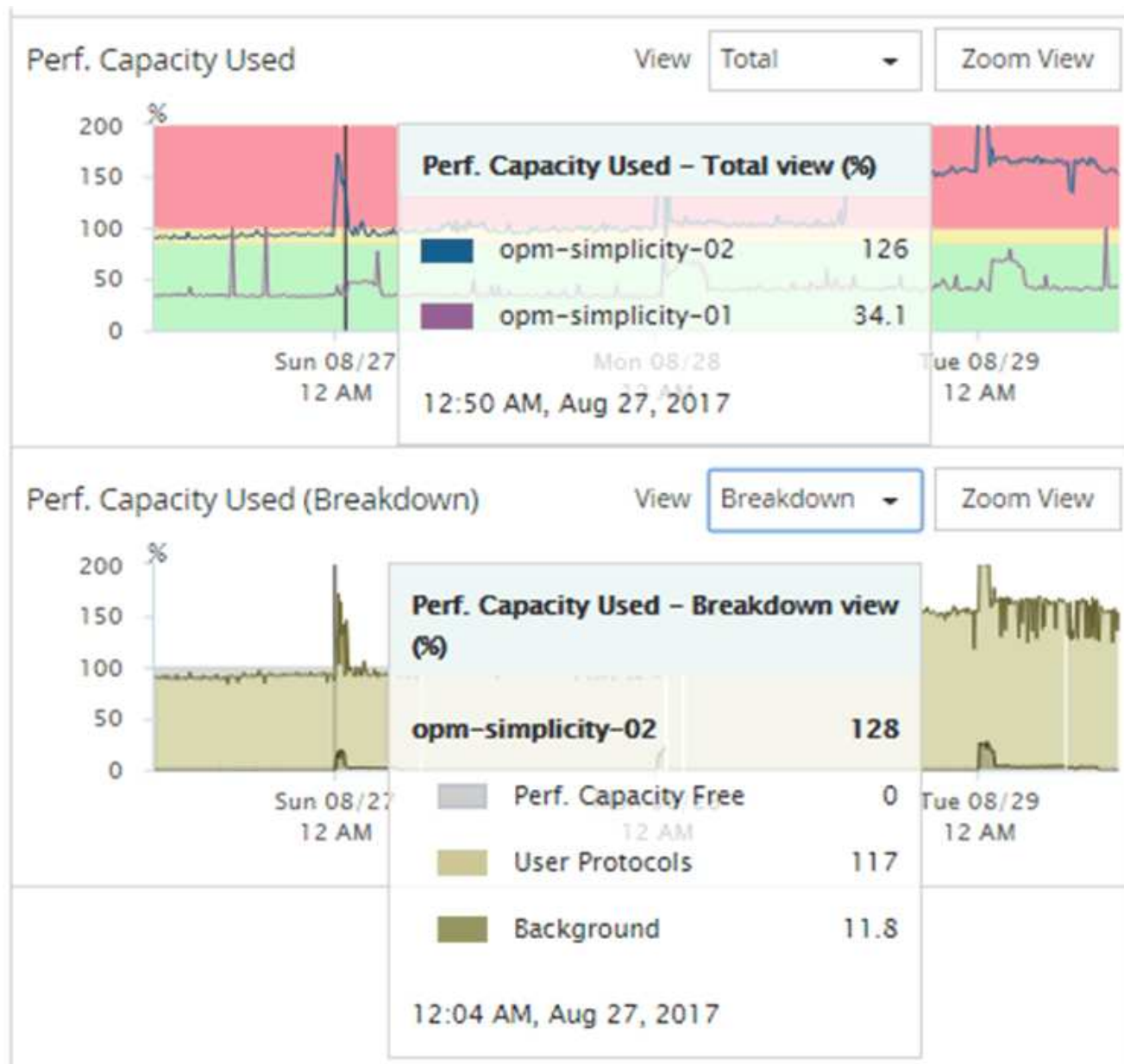


Poiché alcune attività in background associate alla gestione del sistema e dei dati vengono identificate come carichi di lavoro utente e classificate come protocolli utente, la percentuale dei protocolli utente potrebbe apparire artificialmente alta quando tali processi vengono eseguiti. Questi processi vengono solitamente eseguiti intorno a mezzanotte, quando l'utilizzo del cluster è basso. Se si nota un picco nell'attività del protocollo utente intorno a mezzanotte, verificare se i processi di backup del cluster o altre attività in background sono configurati per essere eseguiti in quell'ora.

Passi

1. Selezionare la scheda **Esplora** da un nodo o da una pagina di **Landing** aggregata.
2. Nel riquadro **Grafici contatore**, fare clic su **Scegli grafici**, quindi selezionare **Perf. Tabella della capacità utilizzata**.
3. Scorri verso il basso finché non vedi il grafico.

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 di ripartizione mostra i dettagli dettagliati della capacità prestazionale solo per l'oggetto radice.



4. Per visualizzare uno dei grafici a grandezza naturale, fare clic su **Zoom vista**.

In questo modo è possibile aprire più grafici dei contatori in finestre separate per confrontare i valori della capacità prestazionale utilizzata con i valori IOPS o MBps nello stesso intervallo di tempo.

Capacità prestazionale utilizzata, condizioni di soglia prestazionale

È possibile creare criteri di soglia delle prestazioni definiti dall'utente in modo che gli eventi vengano attivati quando il valore della capacità di prestazioni utilizzata per un nodo o un aggregato supera l'impostazione della soglia della capacità di prestazioni utilizzata definita.

Inoltre, i nodi possono essere configurati con una politica di soglia "Prestazioni capacità utilizzata". Questa politica di soglia somma le statistiche sulla capacità di prestazione utilizzata per entrambi i nodi in una coppia HA per determinare se uno dei due nodi non disporrebbe 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, è

possibile applicare a entrambi i nodi la stessa politica di acquisizione della capacità di prestazioni utilizzata.



Questa equivalenza della capacità di prestazione utilizzata è generalmente vera tra i nodi. Tuttavia, se è presente un traffico tra nodi significativamente maggiore destinato a uno dei nodi tramite il suo partner di failover, la capacità di prestazioni totale utilizzata durante 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 che ha subito l'errore.

Le condizioni di capacità prestazionale utilizzata possono essere utilizzate anche come impostazioni di soglia delle prestazioni secondarie per creare una politica di soglia combinata quando si definiscono soglie per LUN e volumi. La condizione di capacità prestazionale utilizzata viene applicata all'aggregato o al nodo su cui risiede il volume o la LUN. Ad esempio, è possibile creare una politica di soglia combinata utilizzando i seguenti criteri:

Oggetto di archiviazione	Contatore delle prestazioni	Soglia di avvertimento	Soglia critica	Durata
Volume	Latenza	15 ms/operazione	25 ms/operazione	20 minuti
Aggregato	Capacità prestazionale utilizzata	80%	95%	

Le policy di soglia combinate determinano la generazione di un evento solo quando entrambe le condizioni vengono violate per l'intera durata.

Utilizzare il contatore della capacità di prestazione utilizzata per gestire le prestazioni

In genere, le organizzazioni desiderano operare con una percentuale di capacità prestazionale utilizzata inferiore al 100%, in modo che le risorse vengano utilizzate in modo efficiente, riservando al contempo una certa capacità prestazionale aggiuntiva per supportare le richieste dei periodi di picco. È possibile utilizzare criteri di soglia per personalizzare il momento in cui vengono inviati gli avvisi per i valori di capacità ad alte prestazioni utilizzati.

Puoi stabilire obiettivi specifici in base ai tuoi requisiti di prestazione. Ad esempio, le società di servizi finanziari potrebbero riservare una maggiore capacità di performance per garantire l'esecuzione tempestiva delle negoziazioni. Queste aziende potrebbero voler stabilire soglie di capacità prestazionale utilizzata nell'intervallo 70-80 per cento. Le aziende manifatturiere con margini più ridotti potrebbero scegliere di riservare una minore capacità di prestazione se sono disposte a rischiare le prestazioni per gestire meglio i costi IT. Queste aziende potrebbero stabilire soglie di capacità di prestazione utilizzate comprese tra l'85 e il 95 per cento.

Quando il valore della capacità di prestazione utilizzata supera la percentuale impostata in un criterio di soglia definito dall'utente, Unified Manager invia un'e-mail di avviso e aggiunge l'evento alla pagina Inventario eventi. Ciò consente di gestire potenziali problemi prima che incidano sulle prestazioni. Questi eventi possono essere utilizzati anche come indicatori della necessità di apportare modifiche e spostamenti del carico di lavoro all'interno dei nodi e degli aggregati.

Comprendere e utilizzare la pagina Pianificazione del failover dei nodi

La pagina Pianificazione del failover dei nodi/prestazioni stima l'impatto sulle prestazioni di un nodo in caso di guasto del nodo partner ad alta disponibilità (HA). Unified Manager basa le stime sulle prestazioni storiche dei nodi nella coppia HA.

La stima dell'impatto sulle prestazioni di un failover aiuta a pianificare nei seguenti scenari:

- Se un failover riduce sistematicamente le prestazioni stimate del nodo di acquisizione a un livello inaccettabile, è possibile prendere in considerazione l'adozione di misure correttive per ridurre l'impatto sulle prestazioni dovuto al failover.
- Prima di avviare un failover manuale per eseguire attività di manutenzione hardware, è possibile stimare in che modo il failover influisce sulle prestazioni del nodo di acquisizione, per determinare il momento migliore per eseguire l'attività.

Utilizzare la pagina Pianificazione del failover del nodo per determinare le azioni correttive

In base alle informazioni visualizzate nella pagina Pianificazione failover nodi/prestazioni, è possibile adottare misure per garantire che un failover non provochi un calo delle prestazioni di una coppia HA al di sotto di un livello accettabile.

Ad esempio, per ridurre l'impatto stimato sulle prestazioni di un failover, è possibile spostare alcuni volumi o LUN da un nodo nella coppia HA ad altri nodi nel cluster. In questo modo si garantisce che il nodo primario possa continuare a fornire prestazioni accettabili dopo un failover.

Componenti della pagina Pianificazione del failover del nodo

I componenti della pagina Pianificazione del failover dei nodi/prestazioni vengono visualizzati in una griglia e nel riquadro Confronto. Queste sezioni consentono di valutare l'impatto del failover di un nodo sulle prestazioni del nodo di acquisizione.

Griglia delle statistiche delle prestazioni

La pagina Pianificazione del failover dei nodi/prestazioni visualizza una griglia contenente statistiche su latenza, IOPS, utilizzo e capacità prestazionale utilizzata.



I valori di latenza e IOPS visualizzati in questa pagina e nella pagina Prestazioni/Esplora prestazioni nodo potrebbero non corrispondere perché vengono utilizzati contatori delle prestazioni diversi per calcolare i valori per prevedere il failover del nodo.

Nella griglia, a ciascun nodo viene assegnato uno dei seguenti ruoli:

- Primario

Il nodo che subentra al partner HA quando quest'ultimo fallisce. L'oggetto radice è sempre il nodo primario.

- Partner

Il nodo che fallisce nello scenario di failover.

- **Acquisizione stimata**

Lo stesso del nodo primario. Le statistiche sulle prestazioni visualizzate per questo nodo mostrano le prestazioni del nodo di acquisizione dopo aver acquisito il partner non riuscito.



Sebbene il carico di lavoro del nodo di acquisizione sia equivalente ai carichi di lavoro combinati di entrambi i nodi dopo un failover, le statistiche per il nodo di acquisizione stimata 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 Estimated Takeover 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 radice. Dopo aver visualizzato la pagina Performance/Node Performance Explorer, è possibile fare clic sulla scheda **Failover Planning** per vedere come cambiano le prestazioni in questo scenario di errore del nodo. Ad esempio, se Nodo1 è il nodo primario e Nodo2 è il nodo partner, è possibile fare clic su Nodo2 per renderlo primario. In questo modo è possibile vedere come le prestazioni stimate cambiano a seconda del nodo che si guasta.

riquadro di confronto

L'elenco seguente descrive i componenti visualizzati per impostazione predefinita nel riquadro Confronto:

- **Grafici degli eventi**

Vengono visualizzati nello stesso formato di quelli nella pagina Performance/Node Performance Explorer. Riguardano solo il nodo primario.

- **Grafici di contropartita**

Visualizzano le statistiche storiche per il contatore delle prestazioni mostrato nella griglia. In ogni grafico, il grafico per il nodo Takeover stimato mostra le prestazioni stimate se si fosse verificato un failover in un dato momento.

Ad esempio, supponiamo che il grafico di utilizzo mostri il 73% per il nodo di acquisizione stimata alle 11:00 dell'8 febbraio. Se in quel momento si fosse verificato un failover, l'utilizzo del nodo di acquisizione sarebbe stato del 73%.

Le statistiche storiche aiutano a individuare il momento ottimale per avviare un failover, riducendo al minimo la possibilità di sovraccaricare il nodo di acquisizione. È possibile pianificare un failover solo nei momenti in cui le prestazioni previste del nodo di acquisizione sono accettabili.

Per impostazione predefinita, le statistiche per l'oggetto radice e per il nodo partner vengono visualizzate nel riquadro Confronto. A differenza della pagina Performance/Node Performance Explorer, questa pagina non visualizza il pulsante **Aggiungi** per aggiungere oggetti per il confronto delle statistiche.

È possibile personalizzare il riquadro Confronto nello stesso modo in cui si personalizza la pagina Prestazioni/Esplora prestazioni nodo. L'elenco seguente mostra esempi di personalizzazione dei grafici:

- Fare clic sul nome di un nodo per mostrare o nascondere le statistiche del nodo nei grafici Contatore.
- Fare clic su **Zoom vista** per visualizzare un grafico dettagliato per un contatore specifico in una nuova finestra.

Utilizzare una politica di soglia con la pagina Pianificazione del failover del nodo

È possibile creare un criterio di soglia del nodo in modo da ricevere una notifica nella pagina Prestazioni/Pianificazione failover nodo quando un potenziale failover potrebbe ridurre le prestazioni del nodo di acquisizione a un livello inaccettabile.

La soglia di prestazioni definita dal sistema denominata "Coppia di nodi HA sovrautilizzata" genera un evento di avviso se la soglia viene superata per sei periodi di raccolta consecutivi (30 minuti). La soglia è considerata superata se la capacità di prestazioni combinata utilizzata dai nodi in una coppia HA supera il 200%.

L'evento derivante dalla policy di soglia definita dal sistema avvisa che un failover causerà un aumento della latenza del nodo di acquisizione fino a un livello inaccettabile. Quando vedi un evento generato da questa policy per un nodo specifico, puoi passare alla pagina Prestazioni/Pianificazione failover nodo per quel nodo per visualizzare il valore di latenza previsto a causa di un failover.

Oltre a utilizzare questa policy di soglia definita dal sistema, è possibile creare policy di soglia utilizzando il contatore "Capacità di prestazioni utilizzata - Acquisizione" e quindi applicare la policy ai nodi selezionati. Specificando una soglia inferiore al 200% è possibile ricevere un evento prima che venga superata la soglia per la policy definita dal sistema. È anche possibile specificare il periodo di tempo minimo per il quale la soglia viene superata, impostandolo su un valore 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 una policy di soglia per generare un evento di avviso se la capacità di prestazioni combinata utilizzata dai nodi in una coppia HA supera il 175% per più di 10 minuti. È possibile applicare questa policy 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 Pianificazione failover nodi/prestazioni per quel nodo per valutare l'impatto stimato sulle prestazioni del nodo di acquisizione. È possibile adottare misure correttive per evitare di sovraccaricare il nodo di acquisizione in caso di failover. Se si interviene quando la capacità di prestazioni combinata utilizzata dai nodi è inferiore al 200%, la latenza del nodo di acquisizione non raggiunge un livello inaccettabile, anche se durante questo periodo si verifica un failover.

Utilizzare il grafico di ripartizione della capacità di prestazione utilizzata per la pianificazione del failover

Il grafico dettagliato Capacità di prestazione utilizzata - Ripartizione mostra la capacità di prestazione utilizzata per il nodo primario e il nodo partner. Mostra anche la quantità di capacità di prestazioni libera sul nodo Estimated Takeover. Queste informazioni ti aiutano a stabilire se potresti avere un problema di prestazioni in caso di guasto del nodo partner.

Oltre a mostrare la capacità di prestazioni 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 verso e dal cluster.
- I processi in background sono i processi di sistema interni coinvolti nell'efficienza di archiviazione, nella replicazione dei dati e nello stato del sistema.

Questo ulteriore livello di dettaglio consente di determinare se un problema di prestazioni è causato dall'attività dell'applicazione utente o da processi di sistema in background, come la deduplicazione, la ricostruzione RAID, la pulizia del disco e le copie SnapMirror .

Passi

1. Accedere alla pagina **Pianificazione delle prestazioni/failover dei nodi** per il nodo che fungerà da nodo

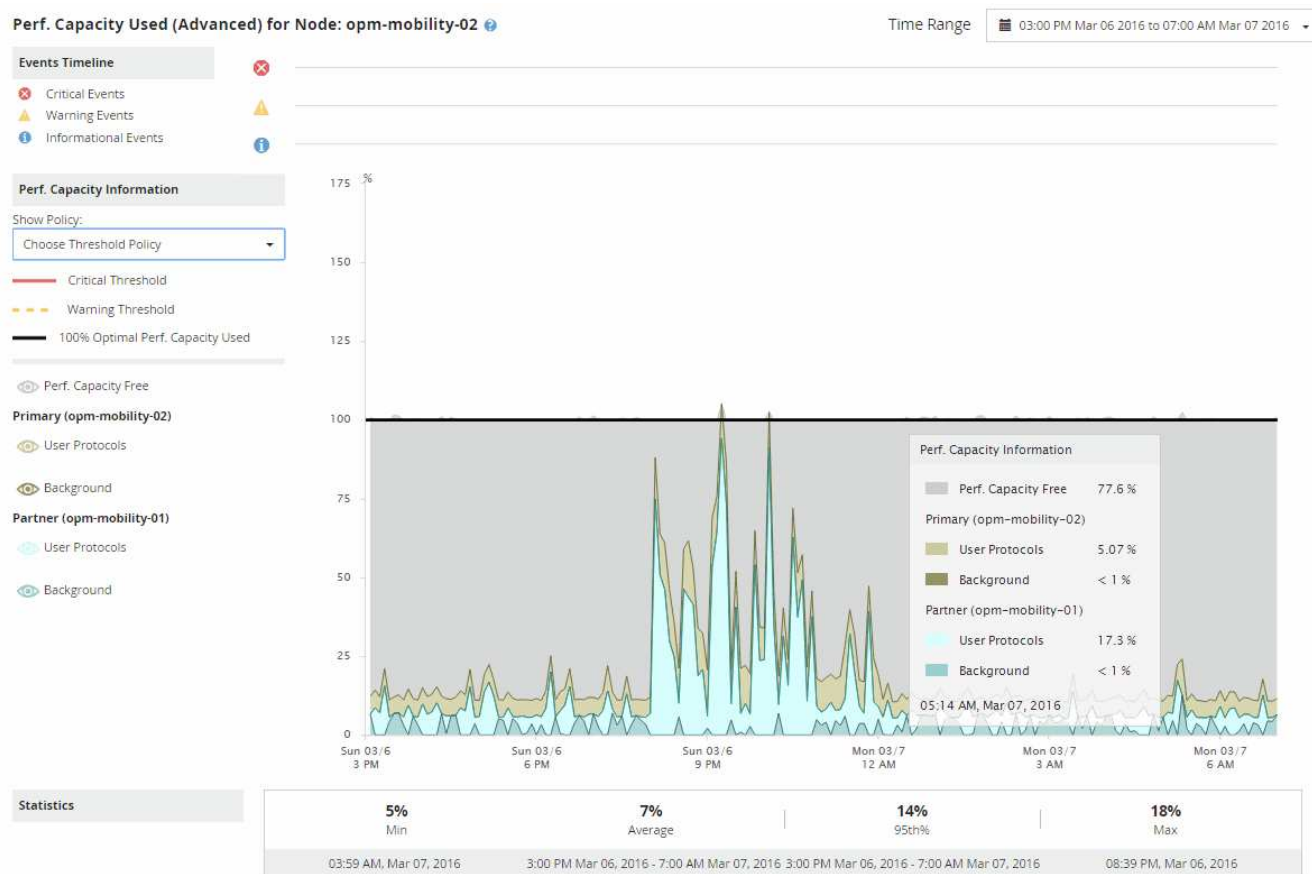
di acquisizione stimata.

2. Dal selettore **Intervallo di tempo**, seleziona il periodo di tempo per il quale visualizzare le statistiche storiche nella griglia del contatore e nei grafici del contatore.

Vengono visualizzati i grafici dei contatori con le statistiche per il nodo primario, il nodo partner e il nodo di acquisizione stimata.

3. Dall'elenco **Scegli grafici**, seleziona **Perf. Capacità utilizzata**.
4. Nella **Perf. Grafico Capacità utilizzata**, selezionare **Ripartizione** e fare clic su **Vista zoom**.

Il grafico dettagliato per Perf. Viene visualizzata la capacità utilizzata.



5. Spostare il cursore sul grafico dettagliato per visualizzare le informazioni sulla capacità prestazionale utilizzata nella finestra popup.

Il Perf. La percentuale di capacità libera è la capacità di prestazione disponibile sul nodo di acquisizione stimata. Indica quanta capacità di prestazioni è rimasta sul nodo di acquisizione dopo un failover. Se è pari a 0%, un failover causerà un aumento della latenza a un livello inaccettabile sul nodo di acquisizione.

6. Valutare l'opportunità di adottare misure correttive per evitare una bassa percentuale di capacità libera di prestazioni.

Se si prevede di avviare un failover per la manutenzione del nodo, scegliere un momento in cui il nodo partner fallisca quando la percentuale di capacità di prestazioni disponibile non è pari a 0.

Raccogli dati e monitora le prestazioni del carico di lavoro

Unified Manager raccoglie e analizza l'attività del carico di lavoro ogni 5 minuti per identificare gli eventi relativi alle prestazioni e rileva le modifiche alla configurazione ogni 15 minuti. Conserva un massimo di 30 giorni di dati storici di 5 minuti sulle prestazioni e sugli eventi e utilizza questi dati per prevedere l'intervallo di latenza previsto per tutti i carichi di lavoro monitorati.

Unified Manager deve raccogliere almeno 3 giorni di attività del carico di lavoro prima di poter iniziare l'analisi e prima che la previsione di latenza per il tempo di risposta I/O possa essere visualizzata nella pagina Analisi del carico di lavoro e nella pagina Dettagli evento. Durante la raccolta di questa attività, la previsione della latenza non visualizza tutte le modifiche che si verificano a causa dell'attività del carico di lavoro. Dopo aver raccolto 3 giorni di attività, Unified Manager modifica la previsione di latenza ogni 24 ore alle 00:00, per riflettere le variazioni dell'attività del carico di lavoro e stabilire una soglia di prestazioni dinamiche più accurata.

Durante i primi 4 giorni in cui Unified Manager monitora un carico di lavoro, se sono trascorse più di 24 ore dall'ultima raccolta dati, i grafici di latenza non visualizzeranno 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, alterando di conseguenza la previsione della latenza delle statistiche sulle prestazioni per i carichi di lavoro monitorati. Unified Manager inizia immediatamente a correggere la previsione di latenza, operazione che richiede circa 15 giorni. Durante questo periodo puoi continuare a utilizzare Unified Manager, ma poiché Unified Manager utilizza la previsione di latenza per rilevare eventi dinamici, alcuni eventi potrebbero non essere accurati. Gli eventi rilevati prima del cambio di orario non sono interessati.

Tipi di carichi di lavoro monitorati da Unified Manager

È possibile utilizzare Unified Manager per monitorare le prestazioni di due tipi di carichi di lavoro: definiti dall'utente e definiti dal sistema.

• **Carichi di lavoro definiti dall'utente**

La velocità di I/O dalle applicazioni al cluster. Si tratta di processi coinvolti nelle richieste di lettura e scrittura. Un volume, una LUN, una condivisione NFS, una condivisione SMB/CIFS e un carico di lavoro sono carichi di lavoro definiti dall'utente.



Unified Manager monitora solo l'attività del carico di lavoro sul cluster. Non monitora le applicazioni, i client o i percorsi tra le applicazioni e il cluster.

Se una o più delle seguenti condizioni sono vere per un carico di lavoro, questo non può essere monitorato 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 di dati offline.
- Si tratta di un volume speculare in una configurazione MetroCluster .

• **Carichi di lavoro definiti dal sistema**

I processi interni coinvolti nell'efficienza di archiviazione, nella replicazione dei dati e nello stato del sistema, tra cui:

- Efficienza di archiviazione, come la deduplicazione
- Integrità del disco, che include la ricostruzione RAID, la pulizia del disco e così via
- Replicazione dei dati, come le copie SnapMirror
- Attività di gestione
- Stato del file system, che include varie attività WAFL
- Scanner del file system, come la scansione WAFL
- Copia offload, ad esempio operazioni di efficienza di archiviazione scaricate dagli host VMware
- Stato di salute del sistema, come spostamenti di volume, compressione dei dati e così via
- Volumi non monitorati

I dati sulle prestazioni per i carichi di lavoro definiti dal sistema vengono visualizzati nell'interfaccia utente grafica solo quando il componente cluster utilizzato da tali carichi di lavoro è in competizione. Ad esempio, non è possibile cercare il nome di un carico di lavoro definito dal sistema per visualizzarne i dati sulle prestazioni nell'interfaccia utente grafica.

Valori di misurazione delle prestazioni del carico di lavoro

Unified Manager misura le prestazioni dei carichi di lavoro su un cluster in base a valori statistici storici e previsti, che costituiscono 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 prestazioni del carico di lavoro sono troppo alte o troppo basse. Un carico di lavoro che non funziona come previsto attiva un evento di prestazioni dinamico per avvisarti.

Nell'illustrazione seguente, il valore effettivo, in rosso, rappresenta le statistiche effettive delle prestazioni nell'intervallo di tempo considerato. Il valore effettivo ha superato la soglia di prestazione, ovvero il limite superiore della latenza prevista. Il picco è il valore effettivo più alto nell'intervallo di tempo. La deviazione misura la variazione tra i valori attesi (previsione) e i valori effettivi, mentre la deviazione massima indica la variazione maggiore tra i valori attesi e i valori effettivi.



Nella tabella seguente sono elencati i valori di misurazione delle prestazioni del carico di lavoro.

Misurazione	Descrizione
Attività	Percentuale del limite QoS utilizzata dai carichi di lavoro nel gruppo di policy.  Se Unified Manager rileva una modifica a un gruppo di policy, ad esempio l'aggiunta o la rimozione di un volume o la modifica del limite 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%.
Attuale	Il valore delle prestazioni misurato in un momento specifico per un dato carico di lavoro.
Deviazione	La variazione tra i valori attesi e i valori effettivi. È il rapporto tra il valore effettivo meno il valore atteso e il valore superiore dell'intervallo atteso meno il valore atteso.  Un valore di deviazione negativo indica che le prestazioni del carico di lavoro sono inferiori alle aspettative, mentre un valore di deviazione positivo indica che le prestazioni del carico di lavoro sono superiori alle aspettative.
Previsto	I valori previsti si basano sull'analisi dei dati storici sulle prestazioni per un dato carico di lavoro. Unified Manager analizza questi valori statistici per determinare l'intervallo previsto (previsione di latenza) dei valori.
Previsione della latenza (intervallo previsto)	La previsione della latenza è una previsione di quali saranno i valori massimi e minimi delle prestazioni previsti in un momento specifico. Per la latenza del carico di lavoro, i valori superiori costituiscono la soglia delle prestazioni. Quando il valore effettivo supera la soglia di prestazione, Unified Manager attiva un evento di prestazione dinamico.
Picco	Il valore massimo misurato in un periodo di tempo.

Misurazione	Descrizione
Deviazione di picco	Il valore massimo della deviazione misurato in un periodo di tempo.
Profondità della coda	Numero di richieste di I/O in sospeso in attesa sul componente di interconnessione.
Utilizzo	Per i componenti di elaborazione di rete, elaborazione dati e aggregazione, la percentuale di tempo impiegato per completare le operazioni del carico di lavoro in un determinato periodo di tempo. Ad esempio, la percentuale di tempo impiegata dai componenti di elaborazione di rete o di elaborazione dati per elaborare una richiesta di I/O o da un aggregato per soddisfare una richiesta di lettura o scrittura.
Velocità di scrittura	Quantità di throughput di scrittura, in megabyte al secondo (MB/s), dai carichi di lavoro su un cluster locale al cluster partner in una configurazione MetroCluster .

Qual è l'intervallo di prestazioni previsto

La previsione della latenza è una previsione di quali saranno i valori massimi e minimi delle prestazioni previsti in un momento specifico. Per la latenza del carico di lavoro, i valori superiori costituiscono la soglia delle prestazioni. Quando il valore effettivo supera la soglia di prestazione, Unified Manager attiva un evento di prestazione dinamico.

Ad esempio, durante il normale orario di lavoro, tra le 9:00 e le 17:00, la maggior parte dei dipendenti potrebbe controllare la posta elettronica tra le 9:00 e le 10:30. L'aumento della domanda sui server di posta elettronica comporta un aumento dell'attività di carico di lavoro sullo storage back-end durante questo periodo. I dipendenti potrebbero notare tempi di risposta lenti nei loro client di posta elettronica.

Durante la pausa pranzo, tra le 12:00 e le 13:00, e alla fine della giornata lavorativa, dopo le 17:00, la maggior parte dei dipendenti è probabilmente lontana dal computer. Solitamente la richiesta sui server di posta elettronica diminuisce, diminuendo anche la richiesta di spazio di archiviazione back-end. In alternativa, potrebbero essere previste operazioni di carico di lavoro programmate, come backup dell'archiviazione o scansioni antivirus, che iniziano dopo le 17:00 e aumentano l'attività sull'archiviazione back-end.

Nel corso di diversi giorni, l'aumento e la diminuzione dell'attività del carico di lavoro determinano l'intervallo previsto (previsione di latenza) dell'attività, con limiti superiori e inferiori per un carico di lavoro. Quando l'attività di carico di lavoro effettivo per un oggetto è al di fuori dei limiti superiori o inferiori e rimane al di fuori di tali limiti per un certo periodo di tempo, ciò potrebbe indicare che l'oggetto è sovrautilizzato o sottoutilizzato.

Come si forma la previsione di latenza

Unified Manager deve raccogliere almeno 3 giorni di attività del carico di lavoro prima di poter 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 a causa dell'attività del

carico di lavoro. Dopo aver raccolto i primi 3 giorni di attività, Unified Manager modifica la previsione di latenza ogni 24 ore alle ore 00:00 per riflettere le variazioni dell'attività del carico di lavoro e stabilire una soglia di prestazioni dinamiche più accurata.



L'ora legale (DST) modifica l'ora del sistema, alterando di conseguenza la previsione della latenza delle statistiche sulle prestazioni per i carichi di lavoro monitorati. Unified Manager inizia immediatamente a correggere la previsione di latenza, operazione che richiede circa 15 giorni. Durante questo periodo puoi continuare a utilizzare Unified Manager, ma poiché Unified Manager utilizza la previsione di latenza per rilevare eventi dinamici, alcuni eventi potrebbero non essere accurati. Gli eventi rilevati prima del cambio di orario non sono interessati.

Come viene utilizzata la previsione della latenza nell'analisi delle prestazioni

Unified Manager utilizza la previsione di latenza per rappresentare l'attività di latenza I/O tipica (tempo di risposta) per i carichi di lavoro monitorati. Ti avvisa quando la latenza effettiva di un carico di lavoro supera i limiti massimi della previsione di latenza, attivando un evento dinamico di prestazioni, in modo da poter analizzare il problema di prestazioni e adottare misure correttive per risolverlo.

La previsione della latenza definisce la base di riferimento delle prestazioni per il carico di lavoro. Nel tempo, Unified Manager impara dalle misurazioni delle prestazioni passate per prevedere i livelli di prestazioni e attività previsti per il carico di lavoro. Il limite superiore dell'intervallo previsto stabilisce la soglia di prestazione dinamica. Unified Manager utilizza la linea di base per determinare quando la latenza effettiva è superiore o inferiore a una soglia oppure al di fuori dei limiti dell'intervallo previsto. Il confronto tra i valori effettivi e quelli previsti crea un profilo delle prestazioni per il carico di lavoro.

Quando la latenza effettiva di un carico di lavoro supera la soglia di prestazioni dinamiche, a causa di una contesa su un componente del cluster, la latenza è elevata e il carico di lavoro funziona più lentamente del previsto. Anche le prestazioni 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 prestazionale. Se l'attività ad alto carico di lavoro rimane costante per un lungo periodo di tempo, ad esempio diverse ore, Unified Manager considera l'attività normale e adatta dinamicamente la previsione di latenza per formare la nuova soglia di prestazioni dinamiche.

Alcuni carichi di lavoro potrebbero avere un'attività costantemente bassa, in cui la latenza prevista non presenta un tasso di variazione elevato nel tempo. Per ridurre al minimo il numero di eventi durante l'analisi degli eventi di prestazioni, Unified Manager attiva un evento solo per i 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 una contesa su un componente del cluster, allora è superiore alla latenza prevista e ha superato la soglia di prestazioni dinamiche.

Quando il traffico di rete diminuisce o il componente del cluster non è più in competizione, la latenza rientra nella previsione di latenza. Se la latenza rimane pari o superiore a 10 ms/op per un lungo periodo di tempo, potrebbe essere necessario adottare misure correttive per risolvere l'evento.

Come Unified Manager utilizza la latenza del carico di lavoro per identificare i problemi di prestazioni

La latenza del carico di lavoro (tempo di risposta) è il tempo impiegato da un volume su un cluster per rispondere alle richieste di I/O provenienti dalle applicazioni client. Unified Manager utilizza la latenza per rilevare eventi relativi alle prestazioni e avvisarti.

Un'elevata latenza significa che le richieste dalle applicazioni a un volume su un cluster impiegano più tempo del solito. La causa dell'elevata latenza potrebbe risiedere nel cluster stesso, a causa di conflitti su uno o più componenti del cluster. Un'elevata latenza potrebbe essere causata anche da problemi esterni al cluster, come colli di bottiglia di rete, problemi con il client che ospita le applicazioni o problemi con le applicazioni stesse.

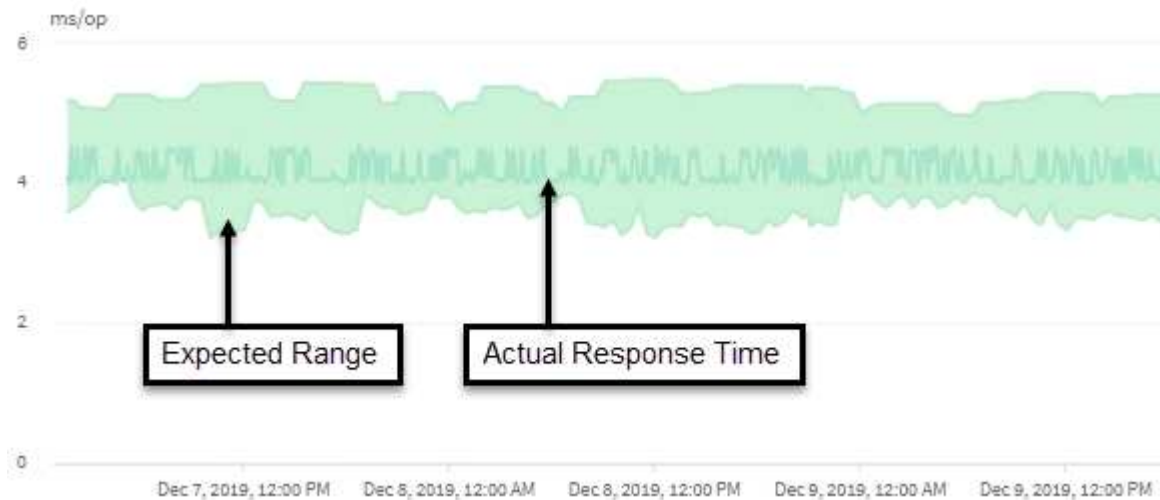


Unified Manager monitora solo l'attività del carico di lavoro sul cluster. Non monitora le applicazioni, i client o i percorsi tra le applicazioni e il cluster.

Anche le operazioni sul cluster, come l'esecuzione di backup o la deduplicazione, che aumentano la richiesta di componenti del cluster condivisi da altri carichi di lavoro, possono contribuire a un'elevata latenza. Se la latenza effettiva supera la soglia di prestazioni dinamiche dell'intervallo previsto (previsione di latenza), Unified Manager analizza l'evento per determinare se si tratta di un evento di prestazioni che potrebbe essere necessario risolvere. La latenza viene misurata in millisecondi per operazione (ms/op).

Nel grafico Latenza totale nella 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 presentano l'attività più elevata o se specifiche operazioni presentano un'attività anomala che influisce sulla latenza di un volume. Quando si analizzano gli eventi relativi alle prestazioni, è possibile utilizzare le statistiche di latenza per determinare se un evento è stato causato da un problema nel cluster. È anche 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 effettiva del tempo di risposta (latenza) è rappresentata da una linea blu, mentre la previsione della latenza (intervallo previsto) è rappresentata da una linea verde.

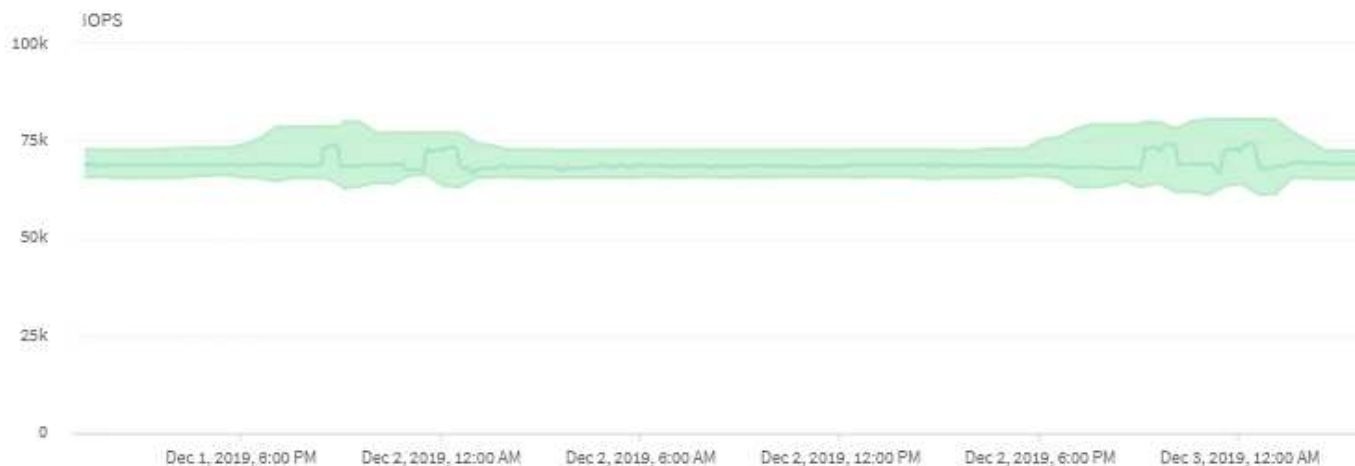


Potrebbero esserci delle lacune nella linea blu se Unified Manager non è riuscito a raccogliere i dati. Ciò può verificarsi perché il cluster o il volume non era raggiungibile, Unified Manager è stato disattivato durante quel periodo oppure la raccolta ha richiesto più tempo dei 5 minuti previsti.

Come le operazioni del cluster possono influenzare la 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 aiutano a determinare se i processi del cluster, come l'esecuzione di backup o la deduplicazione, stanno influenzando la latenza del carico di lavoro (tempo di risposta) o potrebbero aver causato o contribuito a un evento di prestazioni.

Quando si analizzano gli eventi prestazionali, è possibile utilizzare le statistiche IOPS per determinare se un evento prestazionale è stato causato da un problema nel cluster. È possibile identificare le attività specifiche del carico di lavoro che potrebbero aver contribuito in modo significativo all'evento prestazionale. Gli IOPS si misurano in operazioni al secondo (ops/sec).



Questo esempio mostra il grafico IOPS. Le statistiche operative effettive sono rappresentate da una linea blu, mentre le previsioni IOPS delle statistiche operative sono rappresentate da una linea verde.



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 da parte di Unified Manager. È necessario ridurre le risorse utilizzate dal cluster per poter raccogliere le statistiche.

Monitoraggio delle prestazioni delle configurazioni MetroCluster

Unified Manager consente di monitorare la velocità di scrittura tra cluster in una configurazione MetroCluster per identificare i carichi di lavoro con un'elevata velocità di scrittura.

Se questi carichi di lavoro ad alte prestazioni causano tempi di risposta I/O elevati in altri volumi del cluster locale, Unified Manager attiva eventi di prestazioni per avvisarti.



Unified Manager tratta i cluster in una configurazione MetroCluster come cluster individuali. Non distingue tra cluster partner né correla la velocità di scrittura di ciascun cluster.

Quando un cluster locale in una configurazione MetroCluster esegue il mirroring dei propri dati sul cluster partner, i dati vengono scritti nella NVRAM e poi trasferiti tramite i collegamenti interswitch (ISL) agli aggregati remoti. Unified Manager analizza la NVRAM per identificare i carichi di lavoro la cui elevata velocità NVRAM scrittura sta sovrautilizzando la NVRAM, mettendola in competizione.

I carichi di lavoro la cui deviazione nel tempo di risposta ha superato la soglia di prestazioni sono chiamati *vittime*, mentre i carichi di lavoro la cui deviazione nella velocità di scrittura sulla NVRAM è superiore al normale, causando la contesa, sono chiamati *bulli*. Poiché solo le richieste di scrittura vengono replicate nel cluster partner, Unified Manager non analizza la velocità di lettura.

È possibile visualizzare la produttività di uno qualsiasi dei cluster in una configurazione MetroCluster analizzando i carichi di lavoro dei LUN e dei volumi corrispondenti dalle schermate seguenti. È possibile filtrare i risultati in base al cluster. Dal riquadro di navigazione a sinistra:

- Visualizzazione **Archiviazione > Cluster > Prestazioni: Tutti i cluster**. Vedere
- Visualizzazione **Archiviazione > Volumi > Prestazioni: Tutti i volumi**.

- **Archiviazione > LUN > Prestazioni: visualizzazione Tutti i LUN.**
- **Analisi del carico di lavoro > Tutti i carichi di lavoro**

Informazioni correlate

["Analisi e notifica degli eventi prestazionali"](#)

["Analisi degli eventi prestazionali per una configurazione MetroCluster"](#)

["Ruoli dei carichi di lavoro coinvolti in un evento di performance"](#)

["Identificazione dei carichi di lavoro delle vittime coinvolte in un evento di performance"](#)

["Identificazione dei carichi di lavoro impegnativi coinvolti in un evento di performance"](#)

["Identificazione dei carichi di lavoro degli squali coinvolti in un evento di performance"](#)

Comprendere gli eventi e gli avvisi sulle prestazioni

Gli eventi prestazionali sono incidenti correlati alle prestazioni del carico di lavoro su un cluster. Ti aiutano a identificare i carichi di lavoro con tempi di risposta lenti.

Considerando anche gli eventi sanitari verificatisi contemporaneamente, è possibile determinare i problemi che potrebbero aver causato o contribuito ai lenti tempi di risposta.

Quando Unified Manager rileva più occorrenze della stessa condizione di evento per lo stesso componente del cluster, tratta tutte le occorrenze come un singolo evento, non come eventi separati.

È possibile configurare gli avvisi per inviare automaticamente notifiche e-mail quando si verificano eventi di prestazioni di determinati tipi di gravità.

Fonti degli eventi di performance

Gli eventi di prestazione sono problemi relativi alle prestazioni del carico di lavoro su un cluster. Aiutano a identificare gli oggetti di archiviazione con tempi di risposta lenti, noti anche come latenza elevata. Considerando anche altri eventi sanitari verificatisi contemporaneamente, è possibile individuare i problemi che potrebbero aver causato o contribuito alla lentezza dei tempi di risposta.

Unified Manager riceve eventi sulle prestazioni dalle seguenti fonti:

- **Eventi di criteri di soglia delle prestazioni definiti dall'utente**

Problemi di prestazioni basati sui valori di soglia personalizzati impostati. È possibile configurare criteri di soglia delle prestazioni per gli oggetti di archiviazione, ad esempio aggregati e volumi, in modo che vengano generati eventi quando viene superato un valore di soglia per un contatore delle prestazioni.

Per ricevere questi eventi è necessario definire un criterio di soglia delle prestazioni e assegnarlo a un oggetto di archiviazione.

- **Eventi relativi ai criteri di soglia delle prestazioni definiti dal sistema**

Problemi di prestazioni basati su valori soglia definiti dal sistema. Questi criteri di soglia sono inclusi nell'installazione di Unified Manager per coprire i problemi di prestazioni più comuni.

Questi criteri di soglia sono abilitati per impostazione predefinita e potresti visualizzare eventi subito dopo l'aggiunta di un cluster.

- **Eventi di soglia di prestazioni dinamiche**

Problemi di prestazioni derivanti da guasti o errori in un'infrastruttura IT o da carichi di lavoro che sfruttano eccessivamente le risorse del cluster. La causa di questi eventi potrebbe essere un semplice problema che si risolve da solo nel tempo o che può essere risolto con una riparazione o una modifica della configurazione. Un evento di soglia dinamica indica che i carichi di lavoro su un sistema ONTAP sono lenti a causa di altri carichi di lavoro con un utilizzo elevato di componenti cluster condivisi.

Queste soglie sono abilitate per impostazione predefinita e potresti visualizzare eventi dopo tre giorni dalla raccolta dei dati da un nuovo cluster.

Tipi di gravità degli eventi prestazionali

A ogni evento prestazionale è associato un tipo di gravità per aiutarti a stabilire la priorità degli eventi che richiedono un'azione correttiva immediata.

- **Critico**

Si è verificato un evento di prestazione che potrebbe causare un'interruzione del servizio se non si interviene immediatamente con misure correttive.

Gli eventi critici vengono inviati solo da soglie definite dall'utente.

- **Avvertimento**

Un contatore delle prestazioni per un oggetto cluster è fuori dall'intervallo normale e deve essere monitorato per assicurarsi che non raggiunga la gravità critica. Eventi di questa gravità non causano interruzioni del servizio e potrebbero non essere necessarie misure 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 scoperto un nuovo oggetto o quando viene eseguita un'azione da parte dell'utente. Ad esempio, quando viene eliminato un oggetto di archiviazione o quando si verificano modifiche alla configurazione, viene generato l'evento con tipo di gravità Informazioni.

Gli eventi informativi vengono inviati direttamente da ONTAP quando rileva una modifica alla configurazione.

Per maggiori informazioni, consultare i seguenti ["Cosa succede quando viene ricevuto un evento"](#)

* ["Quali informazioni sono contenute in un'e-mail di avviso"](#)

* ["Aggiunta di avvisi"](#)

* ["Aggiunta di avvisi per eventi di performance"](#)

Modifiche alla configurazione rilevate da Unified Manager

Unified Manager monitora i cluster per rilevare eventuali modifiche alla configurazione, aiutandoti a stabilire se una modifica potrebbe aver causato o contribuito a un evento di prestazioni. Le pagine di Performance Explorer visualizzano un'icona di evento di modifica (●) 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 avuto un impatto sulle prestazioni dell'oggetto cluster selezionato. Se la modifica è stata rilevata contemporaneamente o più o meno nello stesso momento di un evento di prestazione, la modifica potrebbe aver contribuito al problema, causando l'attivazione dell'avviso di evento.

Unified Manager può rilevare i seguenti eventi di modifica, classificati come eventi informativi:

- Un volume si sposta tra aggregati.

Unified Manager è in grado di rilevare quando lo spostamento è in corso, completato o fallito. Se Unified Manager è inattivo durante lo spostamento di un volume, quando torna attivo 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 uno o più carichi di lavoro monitorati cambia.

La modifica del limite di un gruppo di policy può causare picchi intermittenti nella latenza (tempo di risposta), che potrebbero anche attivare eventi per il gruppo di policy. La latenza torna gradualmente alla normalità e tutti gli eventi causati dai picchi diventano obsoleti.

- Un nodo in una coppia HA prende il controllo o restituisce lo storage al nodo partner.

Unified Manager è in grado di rilevare quando l'operazione di acquisizione, acquisizione parziale o restituzione è stata completata. Se l'acquisizione è causata da un nodo in panico, Unified Manager non rileva l'evento.

- Un'operazione di aggiornamento o ripristino ONTAP è stata completata correttamente.

Vengono visualizzate la versione precedente e quella nuova.

Tipi di criteri di soglia delle prestazioni definiti dal sistema

Unified Manager fornisce alcuni criteri di soglia standard che monitorano le prestazioni del cluster e generano automaticamente eventi. Questi criteri sono abilitati per impostazione predefinita e generano eventi di avviso o informazione quando vengono superate le soglie di prestazioni monitorate.



I criteri di soglia delle prestazioni 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 prestazioni definito dal sistema, è possibile disattivare gli eventi per i singoli criteri dalla pagina Configurazione evento.

Criteri di soglia del cluster

Per impostazione predefinita, i criteri di soglia delle prestazioni del cluster definiti dal sistema vengono assegnate 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, influenzando potenzialmente le latenze del carico di lavoro.

Ciò avviene confrontando il valore della capacità prestazionale utilizzata per tutti i nodi di un cluster per verificare se un nodo ha superato il valore soglia del 30% per più di 24 ore. Questo è un evento di avvertimento.

- **Squilibrio della capacità del cluster**

Identifica le situazioni in cui un aggregato ha una capacità utilizzata molto più elevata rispetto ad altri aggregati nel cluster e, pertanto, può potenzialmente influire sullo spazio necessario per le operazioni.

Ciò avviene confrontando il valore della capacità utilizzata per tutti gli aggregati nel cluster per verificare se esiste una differenza del 70% tra gli aggregati. Questo è un evento di avvertimento.

Criteri di soglia dei nodi

Per impostazione predefinita, i criteri di soglia delle prestazioni dei nodi definiti dal sistema vengono assegnate a ogni nodo nei cluster monitorati da Unified Manager:

- **Soglia di capacità prestazionale utilizzata superata**

Identifica le situazioni in cui un singolo nodo opera oltre i limiti della sua efficienza operativa, influenzando potenzialmente le latenze del carico di lavoro.

Lo fa cercando i nodi che utilizzano più del 100% della loro capacità prestazionale per più di 12 ore. Questo è un evento di avvertimento.

- **Coppia di nodi HA sovrautilizzata**

Identifica le situazioni in cui i nodi in una coppia HA operano al di sopra dei limiti dell'efficienza operativa della coppia HA.

Ciò avviene esaminando il valore della capacità prestazionale utilizzata per i due nodi nella coppia HA. Se la capacità prestazionale combinata utilizzata dai due nodi supera il 200% per più di 12 ore, un failover del controller avrà un impatto sulle latenze del carico di lavoro. Questo è un evento informativo.

- **Frammentazione del disco del nodo**

Identifica le situazioni in cui un disco o più dischi in un aggregato sono frammentati, rallentando i servizi di sistema chiave e potenzialmente influenzando le latenze del carico di lavoro su un nodo.

Ciò avviene esaminando determinati rapporti di operazioni di lettura e scrittura su tutti gli aggregati su un nodo. Questa policy potrebbe essere attivata anche durante la risincronizzazione SyncMirror o quando vengono rilevati errori durante le operazioni di pulizia del disco. Questo è un evento di avvertimento.



Il criterio "Frammentazione disco nodo" analizza solo gli aggregati HDD; gli aggregati Flash Pool, SSD e FabricPool non vengono analizzati.

Politiche di soglia aggregate

La soglia di prestazioni aggregate definita dal sistema viene assegnata per impostazione predefinita a ogni aggregato nei cluster monitorati da Unified Manager:

• Dischi aggregati sovrautilizzati

Identifica le situazioni in cui un aggregato opera al di sopra dei limiti della sua efficienza operativa, influenzando potenzialmente le latenze del carico di lavoro. Identifica queste situazioni cercando aggregati in cui i dischi nell'aggregato vengono utilizzati per oltre il 95% per più di 30 minuti. Questa policy multi-condizione esegue quindi la seguente analisi per aiutare a determinare la causa del problema:

- Un disco nell'aggregato è attualmente sottoposto ad attività di manutenzione in background?

Alcune delle attività di manutenzione in background a cui potrebbe essere sottoposto un disco sono la ricostruzione del disco, la pulizia del disco, la risincronizzazione SyncMirror e la parity.

- Esiste un collo di bottiglia nelle comunicazioni nell'interconnessione Fibre Channel dello scaffale del disco?
- C'è troppo poco spazio libero nell'aggregato? Un evento di avviso viene emesso per questa policy solo se una (o più) delle tre policy subordinate vengono considerate violate. Un evento di prestazione non viene attivato se solo i dischi nell'aggregato sono utilizzati per più del 95%.



Il criterio "Dischi aggregati sovrautilizzati" analizza gli aggregati solo HDD e gli aggregati Flash Pool (ibridi); gli aggregati SSD e FabricPool non vengono analizzati.

Criteri di soglia di 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 che abbia un criterio di livello di servizio delle prestazioni configurato con un valore di "latenza prevista" definito:

• Soglia di latenza del volume del carico di lavoro/LUN superata come definito dal livello di servizio delle prestazioni

Identifica i volumi (condivisioni file) e le LUN che hanno superato il limite di "latenza prevista" e che influiscono sulle prestazioni del carico di lavoro. Questo è un evento di avvertimento.

Lo fa cercando i carichi di lavoro che hanno superato il valore di latenza previsto per il 30% del tempo durante l'ora precedente.

Criteri di soglia QoS

I criteri di soglia delle prestazioni QoS definiti dal sistema vengono assegnate a qualsiasi carico di lavoro per il quale è configurato un criterio di throughput massimo QoS ONTAP (IOPS, IOPS/TB o MB/s). Unified Manager attiva un evento quando il valore della velocità effettiva del carico di lavoro è inferiore del 15% rispetto al valore QoS configurato:

• Soglia QoS Max IOPS o MB/s

Identifica i volumi e le LUN che hanno superato il limite massimo di IOPS QoS o di throughput MB/s e che influiscono sulla latenza del carico di lavoro. Questo è un evento di avvertimento.

Quando un singolo carico di lavoro viene assegnato a un gruppo di policy, questo avviene cercando i

carichi di lavoro che hanno superato la soglia di throughput massima definita nel gruppo di policy QoS assegnato durante ogni periodo di raccolta per l'ora precedente.

Quando più carichi di lavoro condividono un'unica policy QoS, questa viene eseguita sommando gli IOPS o MB/s di tutti i carichi di lavoro nella policy e confrontando tale totale con la soglia.

- **QoS Picco IOPS/TB o IOPS/TB con soglia di dimensione del blocco**

Identifica i volumi che hanno superato il limite di throughput IOPS/TB di picco QoS adattivo (o IOPS/TB con limite di dimensione del blocco) e che influiscono sulla latenza del carico di lavoro. Questo è un evento di avvertimento.

Ciò avviene convertendo la soglia di picco IOPS/TB definita nella policy QoS adattiva in un valore QoS massimo IOPS basato sulla dimensione di ciascun volume, quindi cerca i volumi che hanno superato il valore QoS massimo IOPS durante ciascun periodo di raccolta delle prestazioni per l'ora precedente.



Questa policy viene applicata ai volumi solo quando il cluster è installato con il software ONTAP 9.3 e versioni successive.

Quando l'elemento "dimensione del blocco" è stato definito nella policy QoS adattiva, la soglia viene convertita in un valore QoS massimo MB/s in base alla dimensione di ciascun volume. Quindi cerca i volumi che hanno superato il QoS max MB/s durante ogni periodo di raccolta delle prestazioni per l'ora precedente.



Questa policy viene applicata ai volumi solo quando il cluster è installato con il software ONTAP 9.5 e versioni successive.

Analisi e notifica degli eventi prestazionali

Gli eventi di prestazione ti informano sui problemi di prestazioni I/O su un carico di lavoro causati da contesa 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 rappresenta ancora un problema che potrebbe essere necessario risolvere.

Unified Manager monitora la latenza I/O (tempo di risposta) e gli IOPS (operazioni) per i volumi su un cluster. Ad esempio, quando altri carichi di lavoro utilizzano eccessivamente un componente del cluster, il componente è in competizione e non riesce a funzionare a un livello ottimale per soddisfare le richieste del carico di lavoro. Le prestazioni di altri carichi di lavoro che utilizzano lo stesso componente potrebbero risentirne, causando un aumento delle latenze. Se la latenza supera la soglia di prestazioni dinamiche, Unified Manager attiva un evento di prestazioni per avvisarti.

Analisi degli eventi

Unified Manager esegue le seguenti analisi, utilizzando le statistiche delle prestazioni dei 15 giorni precedenti, per identificare i carichi di lavoro delle vittime, i carichi di lavoro dei bulli e il componente del cluster coinvolto in un evento:

- Identifica i carichi di lavoro delle vittime la cui latenza ha superato la soglia di prestazioni dinamiche, che rappresenta il limite superiore della previsione di latenza:
 - Per i volumi su aggregati ibridi HDD o Flash Pool (livello locale), gli eventi vengono attivati solo quando la latenza è superiore a 5 millisecondi (ms) e gli IOPS sono superiori a 10 operazioni al secondo (ops/sec).

- Per i volumi su aggregati interamente SSD o aggregati FabricPool (livello cloud), gli eventi vengono attivati solo quando la latenza è superiore a 1 ms e gli IOPS sono superiori a 100 operazioni/sec.
- Identifica il componente del cluster in contesa.



Se la latenza dei carichi di lavoro della vittima nell'interconnessione del cluster è superiore a 1 ms, Unified Manager lo considera significativo e attiva un evento per l'interconnessione del cluster.

- Identifica i carichi di lavoro eccessivi che stanno utilizzando eccessivamente il componente cluster, rendendolo in competizione.
- 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 presentano il cambiamento più elevato nell'utilizzo del componente del cluster e quali vittime sono le più colpite.

Un evento potrebbe verificarsi solo per un breve momento e poi correggersi automaticamente dopo che il componente utilizzato non è più in gioco. Un evento continuo è un evento che si ripete 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.

Una volta risolto, un evento rimane disponibile in Unified Manager come parte del registro dei problemi di prestazioni passati per un volume. Ogni evento ha un ID univoco che identifica il tipo di evento, i volumi, il cluster e i componenti del cluster coinvolti.



Un singolo volume può essere coinvolto in più di un evento 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 riconosciuto). Il problema che ha causato l'evento non è stato risolto o non è stato risolto. Il contatore delle prestazioni per l'oggetto di archiviazione rimane al di sopra della soglia delle prestazioni.

• Obsoleto

Indica che l'evento non è più attivo. Il problema che ha causato l'evento è stato corretto o risolto. Il contatore delle prestazioni per l'oggetto di archiviazione non è più al di sopra della soglia delle prestazioni.

Notifica dell'evento

Gli eventi vengono visualizzati nella pagina Dashboard e in molte altre pagine dell'interfaccia utente e gli avvisi per tali eventi vengono inviati agli indirizzi e-mail specificati. È possibile visualizzare informazioni di analisi dettagliate su un evento e ricevere suggerimenti per risolverlo nella pagina Dettagli evento e nella pagina Analisi carico di lavoro.

Interazione degli eventi

Nella pagina Dettagli evento e nella pagina Analisi carico di lavoro, puoi interagire con gli eventi nei seguenti modi:

- Passando il mouse su un evento viene visualizzato un messaggio che mostra la data e l'ora in cui l'evento è stato rilevato.

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 questione è cerchiato ed evidenziato in rosso. Puoi cliccare su **Visualizza analisi completa** per visualizzare l'analisi completa nella pagina dei dettagli dell'evento. Se sono presenti più eventi per lo stesso periodo di tempo, la finestra di dialogo mostra i dettagli sui tre eventi più recenti. È possibile fare clic su un evento per visualizzarne l'analisi nella pagina Dettagli evento.

Come Unified Manager determina l'impatto sulle prestazioni di un evento

Unified Manager utilizza la deviazione nell'attività, nell'utilizzo, nella velocità di scrittura, nell'utilizzo dei componenti del cluster o nella latenza I/O (tempo di risposta) per un carico di lavoro per determinare il livello di impatto sulle prestazioni del carico di lavoro. Queste informazioni determinano il ruolo di ciascun carico di lavoro nell'evento e la relativa classificazione nella pagina dei dettagli dell'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 i valori analizzati per ultimi e l'intervallo di valori previsto identifica i carichi di lavoro le cui prestazioni sono state maggiormente influenzate dall'evento.

Ad esempio, supponiamo che un cluster contenga due carichi di lavoro: Carico di lavoro A e Carico di lavoro B. La latenza prevista per il Carico di lavoro A è di 5-10 millisecondi per operazione (ms/op) e la latenza effettiva è solitamente di circa 7 ms/op. La latenza prevista per il carico di lavoro B è di 10-20 ms/op, mentre la latenza effettiva è solitamente di circa 15 ms/op. Entrambi i carichi di lavoro rientrano ampiamente nelle previsioni di latenza. A causa della contesa sul cluster, la latenza di entrambi i carichi di lavoro aumenta a 40 ms/op, superando la soglia di prestazioni dinamiche, che rappresenta il limite superiore della previsione di latenza, e innescando eventi. La deviazione della latenza, dai valori previsti ai valori superiori alla soglia di prestazione, per il carico di lavoro A è di circa 33 ms/op, mentre la deviazione per il carico di lavoro B è di circa 25 ms/op. La latenza di entrambi i carichi di lavoro raggiunge un picco di 40 ms/op, ma il carico di lavoro A ha avuto un impatto maggiore sulle prestazioni perché presentava una deviazione di latenza maggiore, pari a 33 ms/op.

Nella pagina Dettagli evento, nella sezione Diagnosi di sistema, è possibile ordinare i carichi di lavoro in base alla deviazione in termini di attività, utilizzo o produttività per un componente del cluster. È anche possibile ordinare i carichi di lavoro in base alla latenza. Quando si seleziona un'opzione di ordinamento, Unified Manager analizza la deviazione in termini di attività, utilizzo, produttività o latenza rispetto ai valori previsti dal momento in cui l'evento è stato rilevato, per determinare l'ordine di ordinamento del carico di lavoro. Per la latenza, i punti rossi (●) indicano il superamento di una soglia di prestazioni da parte di un carico di lavoro vittima e il conseguente impatto sulla latenza. Ogni punto rosso indica un livello di deviazione più elevato nella latenza, che aiuta a 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 competizione

È possibile identificare i problemi di prestazioni del cluster quando un componente del cluster entra in conflitto. Le prestazioni dei carichi di lavoro che utilizzano il componente rallentano e il tempo di risposta (latenza) alle richieste dei client aumenta, il che attiva un evento in Unified Manager.

Un componente in competizione non può funzionare a un livello ottimale. Le sue prestazioni sono diminuite e le prestazioni di altri componenti del cluster e carichi di lavoro, denominati *vittime*, potrebbero aver aumentato la latenza. Per mettere un componente fuori gioco, è necessario ridurre il suo carico di lavoro o aumentare la sua capacità di gestire più lavoro, in modo che le prestazioni possano tornare a livelli normali. Poiché Unified Manager raccoglie e analizza le prestazioni del carico di lavoro a intervalli di cinque minuti, rileva solo quando un componente del cluster viene costantemente sovrautilizzato. Non vengono rilevati picchi transitori di sovrautilizzo che durano solo per un breve periodo nell'intervallo di cinque minuti.

Ad esempio, un aggregato di archiviazione potrebbe essere in competizione perché uno o più carichi di lavoro su di esso competono per soddisfare le loro richieste di I/O. Altri carichi di lavoro sull'aggregato potrebbero essere interessati, con conseguente riduzione delle prestazioni. Per ridurre la quantità di attività sull'aggregato, è possibile adottare diverse misure, ad esempio spostando uno o più carichi di lavoro su un aggregato o un nodo meno occupato, per diminuire la richiesta complessiva di carico di lavoro sull'aggregato corrente. Per un gruppo di policy QoS, è possibile modificare il limite di throughput o spostare i carichi di lavoro in un gruppo di policy diverso, in modo che non vengano più limitati.

Unified Manager monitora i seguenti componenti del cluster per avvisarti quando sono 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 ad attendere il completamento delle transazioni "transfer ready" prima che il cluster possa rispondere a una richiesta di I/O. Se il componente di rete è in competizione, significa che l'elevato tempo di attesa a livello di protocollo sta influenzando la latenza di uno o più carichi di lavoro.

- **Elaborazione di rete**

Rappresenta il componente software nel cluster coinvolto nell'elaborazione I/O tra il livello del protocollo e il cluster. L'elaborazione della rete di gestione del nodo potrebbe essere cambiata da quando è stato rilevato l'evento. Se il componente di elaborazione della rete è in competizione, significa che l'elevato utilizzo del nodo di elaborazione della rete sta influenzando la latenza di uno o più carichi di lavoro.

Quando si utilizza un cluster All SAN Array in una configurazione attiva-attiva, il valore di latenza dell'elaborazione di rete viene visualizzato per entrambi i nodi, in modo da poter verificare che i nodi condividano equamente il carico.

- **Limite QoS massimo**

Rappresenta l'impostazione massima (picco) della velocità effettiva del gruppo di policy QoS (Quality of Service) di archiviazione 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 limitati dal limite di throughput impostato, il che influisce sulla latenza di uno o più di tali carichi di lavoro.

- **Limite QoS minimo**

Rappresenta la latenza di un carico di lavoro causata dall'impostazione minima (prevista) della velocità effettiva QoS assegnata ad altri carichi di lavoro. Se il valore minimo di QoS impostato su determinati carichi di lavoro utilizza la maggior parte della larghezza di banda per garantire la produttività promessa, altri carichi di lavoro saranno limitati e vedranno una maggiore latenza.

- **Interconnessione cluster**

Rappresenta i cavi e gli adattatori con cui i nodi del cluster sono fisicamente collegati. Se il componente di interconnessione del cluster è in conflitto, significa che l'elevato tempo di attesa per le richieste di I/O nell'interconnessione del cluster sta influenzando la latenza di uno o più carichi di lavoro.

- *** Data Processing***

Rappresenta il componente software nel cluster coinvolto nell'elaborazione I/O tra il cluster e l'aggregato di archiviazione 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 dati è in conflitto, significa che l'elevato utilizzo del nodo di elaborazione dati sta influenzando la latenza di uno o più carichi di lavoro.

- **Attivazione del volume**

Rappresenta il processo che tiene traccia dell'utilizzo di tutti i volumi attivi. Negli ambienti di grandi dimensioni in cui sono attivi più di 1000 volumi, questo processo tiene traccia di quanti volumi critici devono accedere alle risorse tramite il nodo contemporaneamente. Quando il numero di volumi attivi contemporaneamente supera la soglia massima consigliata, alcuni volumi non critici subiranno latenza come indicato qui.

- *** Risorse MetroCluster ***

Rappresenta le risorse MetroCluster , tra cui NVRAM e collegamenti interswitch (ISL), utilizzati per eseguire il mirroring dei dati tra cluster in una configurazione MetroCluster . Se il componente MetroCluster è in conflitto, significa che l'elevata velocità di scrittura dei carichi di lavoro sul cluster locale oppure un problema di integrità del collegamento sta influenzando la latenza di uno o più carichi di lavoro sul cluster locale. Se il cluster non è in una configurazione MetroCluster , questa icona non viene visualizzata.

- **Operazioni aggregate o SSD aggregate**

Rappresenta l'aggregato di archiviazione su cui vengono eseguiti i carichi di lavoro. Se il componente aggregato è in competizione, significa che l'elevato utilizzo dell'aggregato sta influenzando la latenza di uno o più carichi di lavoro. Un aggregato è costituito da tutti gli HDD, oppure da un mix di HDD e SSD (un aggregato Flash Pool) oppure da un mix di HDD e un livello cloud (un aggregato FabricPool). Un "aggregato SSD" è costituito da tutti gli SSD (un aggregato all-flash) o da un mix di SSD e un livello cloud (un aggregato FabricPool).

- **Latenza del cloud**

Rappresenta il componente software nel cluster coinvolto nell'elaborazione I/O tra il cluster e il livello cloud su cui sono archiviati i dati utente. Se il componente di latenza del cloud è in conflitto, significa che una grande quantità di letture da volumi ospitati sul livello cloud sta influenzando la latenza di uno o più carichi di lavoro.

- **Sincronizza SnapMirror**

Rappresenta il componente software nel cluster coinvolto nella replica dei dati utente dal volume primario al volume secondario in una relazione sincrona SnapMirror . Se il componente di sincronizzazione SnapMirror è in conflitto, significa che l'attività delle operazioni sincrone SnapMirror sta influenzando la 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 carico di lavoro in un evento di prestazione. I ruoli includono vittime, bulli e squali. Un carico di lavoro definito dall'utente può essere allo stesso tempo vittima, bullo e squalo.

Ruolo	Descrizione
Vittima	Un carico di lavoro definito dall'utente le cui prestazioni sono diminuite a causa di altri carichi di lavoro, denominati "bulli", che utilizzano eccessivamente un componente del cluster. Solo i carichi di lavoro definiti dall'utente vengono identificati come vittime. Unified Manager identifica i carichi di lavoro delle vittime in base alla loro deviazione nella latenza, dove la latenza effettiva, durante un evento, è notevolmente aumentata rispetto alla latenza prevista (intervallo previsto).
Bullo	Un carico di lavoro definito dall'utente o dal sistema il cui utilizzo eccessivo di un componente del cluster ha causato una riduzione delle prestazioni di altri carichi di lavoro, denominati vittime. Unified Manager identifica i carichi di lavoro eccessivi in base alla loro deviazione nell'utilizzo di un componente del cluster, in cui l'utilizzo effettivo, durante un evento, è aumentato notevolmente rispetto all'intervallo di utilizzo previsto.
Squalo	Un carico di lavoro definito dall'utente con il più elevato utilizzo di un componente del cluster rispetto a tutti i carichi di lavoro coinvolti in un evento. Unified Manager identifica i carichi di lavoro degli Shark in base al loro 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 dati e di rete. 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 del carico di lavoro, il componente è in competizione. Il carico di lavoro che comporta l'utilizzo eccessivo di un componente del cluster è un bullo. Le vittime sono gli altri carichi di lavoro che condividono tali componenti e le cui prestazioni sono influenzate dal bullo. Anche le attività derivanti da carichi di lavoro definiti dal sistema, come la deduplicazione o le copie Snapshot, possono degenerare 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 indesiderato che hanno causato l'evento, il componente del cluster in conflitto e i carichi di lavoro vittima le cui prestazioni sono diminuite a causa dell'aumento dell'attività dei carichi di lavoro indesiderato.



Se Unified Manager non riesce a identificare i carichi di lavoro indesiderabili, invia avvisi solo sui carichi di lavoro vittime e sul componente del cluster coinvolto.

Unified Manager è in grado di identificare i carichi di lavoro che sono vittime di carichi di lavoro prepotenti e anche di capire quando questi stessi carichi di lavoro diventano carichi di lavoro prepotenti. Un carico di lavoro può essere un bullo per se stesso. Ad esempio, un carico di lavoro ad alte prestazioni che viene limitato da un limite del gruppo di policy determina la limitazione di tutti i carichi di lavoro nel gruppo di policy, incluso se stesso. Un carico di lavoro che si comporta da bullo o da vittima in un evento di performance in corso potrebbe cambiare il suo ruolo o non partecipare più all'evento.

Gestire le soglie di prestazione

I criteri di soglia delle prestazioni consentono di determinare il punto in cui Unified Manager genera un evento per informare gli amministratori di sistema sui problemi che potrebbero influire sulle prestazioni del carico di lavoro. Queste policy di soglia sono note come soglie di prestazione *definite dall'utente*.

Questa versione supporta soglie di prestazioni definite dall'utente, definite dal sistema e dinamiche. Grazie a soglie di prestazioni dinamiche e definite dal sistema, Unified Manager analizza l'attività del carico di lavoro per determinare il valore di soglia appropriato. Grazie alle soglie definite dall'utente, è possibile definire i limiti massimi delle prestazioni per molti contatori delle prestazioni e per molti oggetti di archiviazione.



Le soglie di prestazioni definite dal sistema e le soglie di prestazioni dinamiche sono impostate da Unified Manager e non sono configurabili. Se si ricevono eventi non necessari da qualsiasi criterio di soglia delle prestazioni definito dal sistema, è possibile disattivare i singoli criteri dalla pagina Configurazione evento.

Come funzionano i criteri di soglia delle prestazioni definiti dall'utente

È possibile impostare criteri di soglia delle prestazioni sugli oggetti di archiviazione (ad esempio, su aggregati e volumi) in modo che un evento possa essere inviato all'amministratore dell'archiviazione per informarlo che il cluster sta riscontrando un problema di prestazioni.

Per creare un criterio di soglia delle prestazioni per un oggetto di archiviazione, procedere come segue:

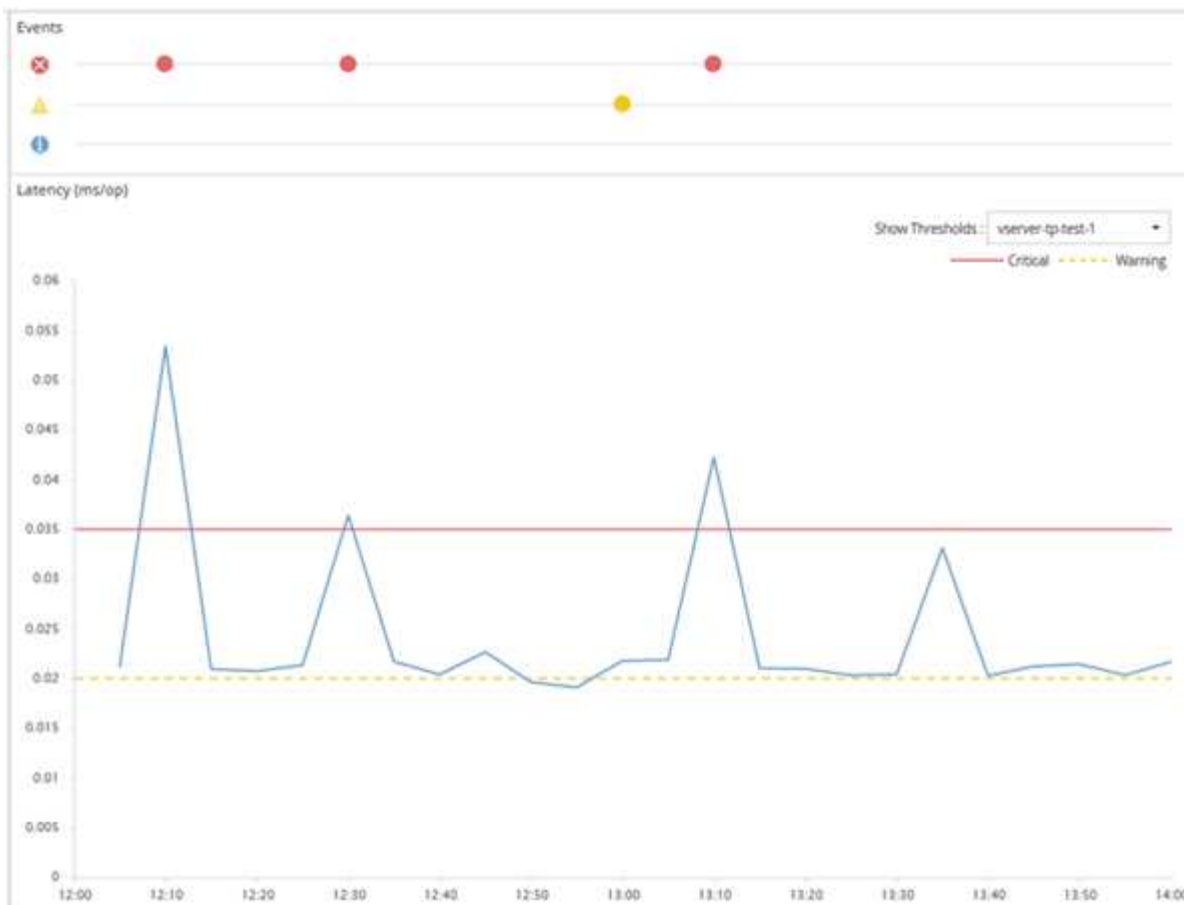
- Selezione di un oggetto di archiviazione
- Selezione di un contatore delle prestazioni associato a quell'oggetto
- Specificare i valori che definiscono i limiti superiori del contatore delle prestazioni considerati situazioni di avviso e critiche
- Specificare un periodo di tempo che definisce per quanto tempo il contatore deve superare il limite superiore

Ad esempio, è possibile impostare un criterio di soglia delle prestazioni su un volume in modo da ricevere una notifica di evento critico ogni volta che gli IOPS per quel volume superano le 750 operazioni al secondo per 10 minuti consecutivi. La stessa policy di soglia può anche specificare che venga inviato un evento di avviso quando gli IOPS superano le 500 operazioni al secondo per 10 minuti.



La versione corrente fornisce soglie che inviano eventi quando il valore di un contatore supera l'impostazione della soglia. Non è possibile impostare soglie che inviano eventi quando il valore di un contatore scende al di sotto di una soglia impostata.

Di seguito è riportato un esempio di grafico contatore, che indica che una soglia di avviso (icona gialla) è stata superata alle 1:00 e che una soglia critica (icona rossa) è stata superata alle 12:10, 12:30 e 1:10:



La violazione della soglia deve verificarsi in modo continuativo per la durata specificata. Se per qualsiasi motivo la soglia scende al di sotto dei valori limite, una successiva violazione è considerata l'inizio di una nuova durata.

Alcuni oggetti cluster e contatori delle prestazioni consentono di creare una policy di soglia combinata che richiede che due contatori delle prestazioni superino i loro 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 prestazioni	Soglia di avvertimento	Soglia critica	Durata
Volume	Latenza	10 millisecondi	20 millisecondi	15 minuti
Aggregato	Utilizzo	65%	85%	

Le policy di soglia che utilizzano due oggetti cluster determinano la generazione di un evento solo quando entrambe le condizioni vengono violate. Ad esempio, utilizzando la politica di soglia definita nella tabella:

Se la latenza del volume è media...	E l'utilizzo aggregato del disco è...	Poi...
15 millisecondi	50%	Non è stato segnalato alcun evento.

Se la latenza del volume è media...	E l'utilizzo aggregato del disco è...	Poi...
15 millisecondi	75%	È stato segnalato un evento di avviso.
25 millisecondi	75%	È stato segnalato un evento di avviso.
25 millisecondi	90%	È stato segnalato un evento critico.

Cosa succede quando viene violata una soglia di prestazione

Quando il valore di un contatore supera il valore soglia delle prestazioni definito per il periodo di tempo specificato nella durata, la soglia viene superata e viene segnalato un evento.

L'evento determina l'avvio delle seguenti azioni:

- L'evento viene visualizzato nella Dashboard, nella pagina Riepilogo cluster prestazioni, nella pagina Eventi e nella pagina Inventario prestazioni specifica dell'oggetto.
- (facoltativo) È possibile inviare un avviso e-mail sull'evento a uno o più destinatari e-mail e una trap SNMP può essere inviata a un ricevitore di trap.
- (facoltativo) È possibile eseguire uno script per modificare o aggiornare automaticamente gli oggetti di archiviazione.

La prima azione viene sempre eseguita. È possibile configurare se le azioni facoltative devono essere eseguite nella pagina Impostazione avvisi. È possibile definire azioni univoche a seconda che venga violata una soglia di avviso o di soglia critica.

Dopo che si è verificata una violazione della soglia di prestazione su un oggetto di archiviazione, non vengono generati ulteriori eventi per tale soglia finché il valore del contatore non scende al di sotto del valore di soglia, momento in cui la durata per tale limite viene reimpostata. Finché la soglia continua a essere superata, l'ora di fine dell'evento viene continuamente aggiornata per indicare che l'evento è in corso.

Un evento soglia cattura o blocca le informazioni relative alla gravità e alla definizione della policy, in modo che con l'evento vengano visualizzate informazioni univoche sulla soglia, anche se la policy sulla soglia viene modificata in futuro.

Quali contatori delle prestazioni possono essere monitorati utilizzando le soglie

Alcuni contatori di prestazioni comuni, come IOPS e MB/s, possono avere soglie impostate per tutti gli oggetti di archiviazione. Esistono altri contatori per i quali è possibile impostare soglie solo per determinati oggetti di archiviazione.

Contatori di prestazioni disponibili

Oggetto di archiviazione	Contatore delle prestazioni	Descrizione
Grappolo	IOPS	Numero medio di operazioni di input/output elaborate dal cluster al secondo.
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 elaborate dal nodo al secondo.	MB/s
Numero medio di megabyte di dati trasferiti da e verso questo nodo al secondo.	Latenza	Numero medio di millisecondi impiegati dal nodo per rispondere alle richieste dell'applicazione.
Utilizzo	Percentuale media della CPU e della RAM del nodo utilizzata.	Capacità di prestazione utilizzata
Percentuale media della capacità di prestazione consumata dal nodo.	Capacità di prestazione utilizzata - Acquisizione	Percentuale media della capacità di prestazione consumata dal nodo, più la capacità di prestazione del nodo partner.
Aggregato	IOPS	Numero medio di operazioni di input/output elaborate dall'aggregato al secondo.
MB/s	Numero medio di megabyte di dati trasferiti da e verso questo aggregato al secondo.	Latenza
Numero medio di millisecondi impiegati dall'aggregato per rispondere alle richieste dell'applicazione.	Utilizzo	Percentuale media dei dischi dell'aggregato utilizzati.
Capacità di prestazione utilizzata	Percentuale media della capacità prestazionale consumata dall'aggregato.	VM di archiviazione
IOPS	Numero medio di operazioni di input/output elaborate dall'SVM al secondo.	MB/s

Oggetto di archiviazione	Contatore delle prestazioni	Descrizione
Numero medio di megabyte di dati trasferiti da e verso questa SVM al secondo.	Latenza	Numero medio di millisecondi impiegati dall'SVM per rispondere alle richieste dell'applicazione.
Volume	IOPS	Numero medio di operazioni di input/output elaborate dal volume al secondo.
MB/s	Numero medio di megabyte di dati trasferiti da e verso questo volume al secondo.	Latenza
Numero medio di millisecondi impiegati dal volume per rispondere alle richieste dell'applicazione.	Rapporto di mancata memorizzazione nella cache	Percentuale media di richieste di lettura da applicazioni client restituite dal volume anziché dalla cache.
LUN	IOPS	Numero medio di operazioni di input/output elaborate dalla LUN al secondo.
MB/s	Numero medio di megabyte di dati trasferiti da e verso questa LUN al secondo.	Latenza
Numero medio di millisecondi impiegati dalla LUN per rispondere alle richieste dell'applicazione.	Spazio dei nomi	IOPS
Numero medio di operazioni di input/output elaborate dallo spazio dei nomi al secondo.	MB/s	Numero medio di megabyte di dati trasferiti da e verso questo namespace al secondo.
Latenza	Numero medio di millisecondi impiegati dallo 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 nelle policy di soglia combinate

Solo alcuni contatori delle prestazioni possono essere utilizzati insieme nelle policy combinate. Quando vengono specificati contatori delle prestazioni primari e secondari, entrambi i contatori delle prestazioni devono superare i loro limiti massimi prima che venga generato un evento.

Oggetto di archiviazione primario e contatore	Oggetto di archiviazione secondario e contatore
Latenza del volume	IOPS volume
Volume MB/s	Utilizzo aggregato
Capacità di prestazione aggregata utilizzata	Utilizzo del nodo
Capacità di prestazioni del nodo utilizzata	Capacità di prestazione del nodo utilizzata - Acquisizione
Latenza LUN	LUN IOPS
MB/s LUN	Utilizzo aggregato
Capacità di prestazione aggregata utilizzata	Utilizzo del nodo
Capacità di prestazioni del nodo utilizzata	Capacità di prestazione del nodo utilizzata - Acquisizione



Quando un criterio di combinazione di volumi viene applicato a un volume FlexGroup , anziché a un FlexVol volume, solo gli attributi “Volume IOPS” e “Volume MB/s” possono essere selezionati come contatore secondario. Se il criterio di soglia contiene uno degli attributi nodo o aggregato, il criterio non verrà applicato al volume FlexGroup e verrà visualizzato un messaggio di errore che descrive questo caso. Ciò avviene perché i volumi FlexGroup possono esistere su più nodi o aggregati.

Creare criteri di soglia delle prestazioni definiti dall'utente

È possibile creare criteri di soglia delle prestazioni per gli oggetti di archiviazione in modo che vengano inviate notifiche quando un contatore delle prestazioni supera un valore specifico. La notifica dell'evento indica che il cluster sta riscontrando un problema di prestazioni.

Prima di iniziare

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 nuove policy definendo tutti i valori delle policy in questa pagina oppure è possibile creare una copia di una policy esistente e modificare i valori nella copia (operazione denominata *clonazione*).

I valori di soglia validi sono compresi tra 0,001 e 10.000.000 per i numeri, tra 0,001 e 100 per le percentuali e tra 0,001 e 200 per le percentuali di capacità di prestazione utilizzata.



La versione corrente fornisce soglie che inviano eventi quando il valore di un contatore supera l'impostazione della soglia. Non è possibile impostare soglie che inviano eventi quando il valore di un contatore scende al di sotto di una soglia impostata.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Soglie eventi > Prestazioni**.

Viene visualizzata la pagina Soglie di prestazione.

2. Fare clic sul pulsante appropriato a seconda che si desideri creare una nuova policy o clonare una policy simile e modificare la versione clonata.

A...	Clic...
Crea una nuova politica	Creare
Clona una policy esistente	Seleziona una policy esistente e fai clic su Clona

Viene visualizzata la pagina Crea criterio soglia prestazioni o Clona criterio soglia prestazioni.

3. Definisci la policy di soglia specificando i valori di soglia del contatore delle prestazioni che desideri impostare per oggetti di archiviazione specifici:

- a. Selezionare il tipo di oggetto di archiviazione e specificare un nome e una descrizione per il criterio.
- b. Selezionare il contatore delle prestazioni da monitorare e specificare i valori limite che definiscono gli eventi di avviso e critici.

È necessario definire almeno un limite di avviso o un limite critico. Non è necessario definire entrambi i tipi di limiti.

- c. Selezionare un contatore delle prestazioni secondario, se necessario, e specificare i valori limite per gli eventi di avviso e critici.

Per includere un contatore secondario è necessario che entrambi i contatori superino i valori limite prima che la soglia venga superata e venga segnalato un evento. Solo determinati oggetti e contatori possono essere configurati utilizzando una policy di combinazione.

- d. Selezionare la durata di tempo per la quale i valori limite devono essere superati affinché venga inviato un evento.

Quando si clona una policy esistente, è necessario immettere un nuovo nome per la policy.

4. Fare clic su **Salva** per salvare la policy.

Verrai reindirizzato alla pagina Soglie di prestazione. Un messaggio di successo nella parte superiore della pagina conferma che il criterio di soglia è stato creato e fornisce un collegamento alla pagina Inventario per quel tipo di oggetto, in modo da poter applicare immediatamente il nuovo criterio agli oggetti di archiviazione.

Se si desidera applicare la nuova politica di soglia agli oggetti di archiviazione in questo momento, è possibile

fare clic sul collegamento **Vai a object_type ora** per andare alla pagina Inventario.

Assegnare criteri di soglia delle prestazioni agli oggetti di archiviazione

È possibile assegnare un criterio di soglia delle prestazioni definito dall'utente a un oggetto di archiviazione in modo che Unified Manager segnali un evento se il valore del contatore delle prestazioni supera l'impostazione del criterio.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Devono esistere i criteri di soglia delle prestazioni che si desidera applicare all'oggetto.

È possibile applicare solo un criterio di prestazione 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 archiviazione. Quando si assegnano policy a più oggetti, se a uno degli oggetti è già assegnato il numero massimo di policy, Unified Manager esegue le seguenti azioni:

- Applica la policy a tutti gli oggetti selezionati che non hanno raggiunto il loro massimo
- Ignora gli oggetti che hanno raggiunto il numero massimo di policy
- Visualizza un messaggio che indica che il criterio non è stato assegnato a tutti gli oggetti

Passi

1. Dalla pagina Inventario delle prestazioni di qualsiasi oggetto di archiviazione, seleziona l'oggetto o gli oggetti a cui desideri assegnare un criterio di soglia:

Per assegnare soglie a...	Clic...
Un singolo oggetto	La casella di controllo a sinistra di quell'oggetto.
Oggetti multipli	La casella di controllo a sinistra di ogni oggetto.
Tutti gli oggetti sulla pagina	IL  casella a discesa e scegliere Seleziona tutti gli oggetti in questa pagina.
Tutti gli oggetti dello stesso tipo	IL  casella a discesa e scegliere Seleziona tutti gli oggetti.

È possibile utilizzare la funzionalità di ordinamento e filtraggio per perfezionare l'elenco degli oggetti nella pagina dell'inventario e semplificare l'applicazione di criteri di soglia a molti oggetti.

2. Effettua la tua selezione, quindi fai clic su **Assegna criterio soglia prestazioni**.

Viene visualizzata la pagina Assegna criterio soglia prestazioni, che mostra un elenco dei criteri soglia esistenti per quel tipo specifico di oggetto di archiviazione.

3. Fare clic su ciascun criterio per visualizzare i dettagli delle impostazioni della soglia delle prestazioni per verificare di aver selezionato il criterio di soglia corretto.
4. Dopo aver selezionato il criterio di soglia appropriato, fare clic su **Assegna criterio**.

Un messaggio di conferma 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 di avviso per questo oggetto e criterio.

Se si desidera ricevere avvisi tramite e-mail o come trap SNMP per essere informati che è stato generato un particolare evento di prestazione, è necessario configurare le impostazioni di avviso nella pagina Configurazione avviso.

Visualizza i criteri di soglia delle prestazioni

È possibile visualizzare tutti i criteri di soglia delle prestazioni attualmente definiti dalla pagina Soglie delle prestazioni.

L'elenco delle policy di soglia è ordinato alfabeticamente in base al nome della policy e include policy per tutti i tipi di oggetti di archiviazione. È possibile fare clic sull'intestazione di una colonna per ordinare le policy in base a quella colonna. Se stai cercando una policy specifica, utilizza i meccanismi di filtro e ricerca per restringere l'elenco delle policy di soglia visualizzate nell'elenco dell'inventario.

È possibile passare il cursore sul Nome della policy e sul Nome della condizione per visualizzare i dettagli di configurazione della policy. Inoltre, è possibile utilizzare i pulsanti forniti per creare, clonare, modificare ed eliminare criteri di soglia definiti dall'utente.

Fare un passo

1. Nel riquadro di navigazione a sinistra, seleziona **Soglie eventi > Prestazioni**.

Viene visualizzata la pagina Soglie di prestazione.

Modificare i criteri di soglia delle prestazioni definiti dall'utente

È possibile modificare le impostazioni di soglia per i criteri di soglia delle prestazioni esistenti. Questa funzionalità può essere utile se si riscontra di ricevere troppi o troppo pochi avvisi per determinate condizioni di soglia.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Non è possibile modificare il nome del criterio o il tipo di oggetto di archiviazione monitorato per i criteri di soglia esistenti.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Soglie eventi > Prestazioni**.

Viene visualizzata la pagina Soglie di prestazione.

2. Selezionare la soglia che si desidera modificare e fare clic su **Modifica**.

Viene visualizzata la pagina Modifica criterio soglia prestazioni.

3. Apporta le modifiche alla policy di soglia e fai clic su **Salva**.

Verrai reindirizzato alla pagina Soglie di prestazione.

Dopo il salvataggio, le modifiche vengono aggiornate immediatamente su tutti gli oggetti di archiviazione che utilizzano il criterio.

A seconda del tipo di modifiche apportate al criterio, potrebbe essere necessario rivedere le impostazioni di avviso configurate per gli oggetti che utilizzano il criterio nella pagina Impostazione avviso.

Rimuovere i criteri di soglia delle prestazioni dagli oggetti di archiviazione

È possibile rimuovere un criterio di soglia delle prestazioni definito dall'utente da un oggetto di archiviazione quando non si desidera più che Unified Manager monitori il valore del contatore delle prestazioni.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

È possibile rimuovere solo un criterio alla volta da un oggetto selezionato.

È possibile rimuovere un criterio di soglia da più oggetti di archiviazione selezionando più di un oggetto nell'elenco.

Passi

1. Dalla pagina **inventario** di qualsiasi oggetto di archiviazione, seleziona uno o più oggetti a cui è applicata almeno una policy di soglia delle prestazioni.

Per cancellare le soglie da...	Fai questo...
Un singolo oggetto	Seleziona la casella di controllo a sinistra dell'oggetto.
Oggetti multipli	Selezionare la casella di controllo a sinistra di ciascun oggetto.
Tutti gli oggetti sulla pagina	Clic  nell'intestazione della colonna.

2. Fare clic su **Cancella criterio soglia prestazioni**.

Viene visualizzata la pagina Cancella criterio soglia, che mostra un elenco dei criteri soglia attualmente assegnati agli oggetti di archiviazione.

3. Selezionare la policy di soglia che si desidera rimuovere dagli oggetti e fare clic su **Cancella 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 succede quando viene modificata una politica di soglia di prestazione

Se si modifica 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 archiviazione che utilizzano il criterio. La nuova impostazione viene applicata immediatamente e Unified Manager inizia a confrontare i valori del contatore delle prestazioni con le nuove

impostazioni di soglia per tutti i dati sulle prestazioni appena raccolti.

Se sono presenti eventi attivi per oggetti che utilizzano la policy di soglia modificata, gli eventi vengono contrassegnati come obsoleti e la policy di soglia inizia a monitorare il contatore come una policy di soglia appena definita.

Quando si visualizza il contatore a cui è stata applicata la soglia nella vista dettagliata dei grafici dei contatori, le linee delle soglie critiche e di avviso riflettono le impostazioni correnti delle soglie. Le impostazioni di soglia originali non vengono visualizzate in questa pagina, anche se si visualizzano i dati storici relativi al periodo in cui era in vigore la vecchia impostazione di soglia.



Poiché le impostazioni di soglia precedenti non vengono visualizzate nella vista dettagliata dei grafici dei contatori, potresti vedere eventi storici che compaiono al di sotto delle linee di soglia correnti.

Cosa succede alle policy di soglia delle prestazioni quando un oggetto viene spostato

Poiché i criteri di soglia delle prestazioni vengono assegnate agli oggetti di archiviazione, se si sposta un oggetto, tutti i criteri di soglia assegnati rimangono associati all'oggetto una volta completato lo spostamento. Ad esempio, se si sposta un volume o una LUN in un aggregato diverso, i criteri di soglia rimangono attivi per il volume o la LUN nel nuovo aggregato.

Se esiste una condizione di contatore secondaria per la policy di soglia (una policy di combinazione), ad esempio se una condizione aggiuntiva è assegnata a un aggregato o a un nodo, la condizione di contatore secondaria viene applicata al nuovo aggregato o nodo in cui è stato spostato il volume o la LUN.

Se sono presenti nuovi eventi attivi per gli oggetti che utilizzano la policy di soglia modificata, gli eventi vengono contrassegnati come obsoleti e la policy di soglia inizia a monitorare il contatore come una policy di soglia appena definita.

Un'operazione di spostamento del volume fa sì che ONTAP invii un evento di modifica informativo. Un'icona di evento di modifica viene visualizzata nella cronologia Eventi nella pagina Performance Explorer e nella pagina Workload Analysis per indicare l'ora in cui è stata completata l'operazione di spostamento.



Se si sposta un oggetto in un cluster diverso, la policy di soglia definita dall'utente viene rimossa dall'oggetto. Se necessario, è necessario assegnare un criterio di soglia all'oggetto dopo il completamento dell'operazione di spostamento. I criteri di soglia dinamici e definiti dal sistema, invece, vengono applicati automaticamente a un oggetto dopo che è stato spostato in un nuovo cluster.

Funzionalità della politica di soglia durante l'acquisizione e la restituzione dell'HA

Quando si verifica un'operazione di acquisizione o restituzione in una configurazione ad alta disponibilità (HA), gli oggetti che vengono 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 sia un'operazione di acquisizione che di restituzione entro il periodo di raccolta delle modifiche alla configurazione di 15 minuti, è possibile che le statistiche sulle prestazioni non vengano spostate da un nodo all'altro.

Funzionalità della politica di soglia durante la rilocalizzazione aggregata

Se si sposta un aggregato da un nodo a un altro nodo utilizzando `aggregate relocation start` comando, sia le policy di soglia singole che quelle combinate vengono mantenute su tutti gli oggetti e la parte del nodo della policy di soglia viene applicata al nuovo nodo.

Funzionalità della politica di soglia durante il passaggio a 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 sui volumi e sulle LUN spostati nel cluster partner. Dopo che un oggetto è stato riportato al suo cluster originale, la politica di soglia definita dall'utente viene riapplicata automaticamente.

Per informazioni, vedere ["Comportamento del volume durante la commutazione e la commutazione indietro"](#).

Analizza gli eventi di performance

È possibile analizzare gli eventi di prestazioni 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 risolvere autonomamente gli eventi.

Visualizza informazioni sugli eventi di performance

È possibile utilizzare la pagina dell'inventario di Gestione eventi per visualizzare un elenco di tutti gli eventi di prestazioni sui cluster monitorati da Unified Manager. Visualizzando queste informazioni è possibile individuare gli eventi più critici e quindi analizzare le informazioni dettagliate per determinare la causa dell'evento.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

L'elenco degli eventi è ordinato in base all'ora di rilevamento, con gli eventi più recenti elencati per primi. È possibile fare clic sull'intestazione di una colonna per ordinare gli eventi in base a quella colonna. Ad esempio, è possibile ordinare in base alla colonna Stato per visualizzare gli eventi in base alla gravità. Se stai cercando un evento specifico o un tipo specifico di evento, puoi utilizzare i meccanismi di filtro e ricerca per restringere l'elenco degli eventi visualizzati.

In questa pagina vengono visualizzati gli eventi provenienti da tutte le fonti:

- Criterio di soglia delle prestazioni definito dall'utente
- Criterio di soglia delle prestazioni definito dal sistema
- Soglia di prestazione dinamica

Nella colonna Tipo di evento è elencata l'origine dell'evento. Puoi selezionare un evento per visualizzarne i dettagli nella pagina Dettagli evento.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.
2. Dal menu Visualizza, seleziona **Eventi prestazioni attivi**.

La pagina mostra tutti gli eventi di prestazioni nuovi e riconosciuti generati negli ultimi 7 giorni.

3. Individua l'evento che desideri analizzare e fai clic sul nome dell'evento.

Viene visualizzata la pagina dei dettagli dell'evento.



È anche possibile visualizzare la pagina dei dettagli di un evento facendo clic sul collegamento al nome dell'evento nella pagina Performance Explorer e in un'e-mail di avviso.

Analizza gli eventi dalle soglie di prestazioni definite dall'utente

Gli eventi generati dalle soglie definite dall'utente indicano che un contatore delle prestazioni per un determinato oggetto di archiviazione, ad esempio un aggregato o un volume, ha superato la soglia definita nel criterio. Ciò indica che l'oggetto cluster sta riscontrando un problema di prestazioni.

È possibile utilizzare la pagina Dettagli evento per analizzare l'evento prestazionale e, se necessario, adottare misure correttive per riportare le prestazioni alla normalità.

Rispondere agli eventi di soglia delle prestazioni definiti dall'utente

È possibile utilizzare Unified Manager per analizzare gli eventi relativi alle prestazioni causati dal superamento da parte di un contatore delle prestazioni di una soglia di avviso o critica definita dall'utente. È anche possibile utilizzare Unified Manager per verificare lo stato di integrità del componente del cluster e verificare se gli eventi di integrità recenti rilevati sul componente hanno contribuito all'evento relativo alle prestazioni.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance nuovi o obsoleti.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Esaminare la **Descrizione**, che descrive la violazione della soglia che ha causato l'evento.

Ad esempio, il messaggio "Un valore di latenza di 456 ms/op ha attivato un evento di AVVISO in base all'impostazione della soglia di 400 ms/op" indica che si è verificato un evento di avviso di latenza per l'oggetto.

3. Passa il cursore sul nome della policy per visualizzare i dettagli sulla policy di soglia che ha attivato l'evento.

Ciò include il nome della policy, il contatore delle prestazioni in fase di valutazione, il valore del contatore

che deve essere superato per essere considerato un evento critico o di avviso e la durata entro la quale il contatore deve superare il valore.

4. Prendi nota dell'**Ora di attivazione dell'evento** in modo da poter verificare se altri eventi potrebbero essersi verificati contemporaneamente e aver contribuito a questo evento.
5. Per analizzare ulteriormente l'evento e determinare se è necessario eseguire azioni per risolvere il problema di prestazioni, seguire una delle opzioni seguenti:

Opzione	Possibili azioni di indagine
Fare clic sul nome dell'oggetto Sorgente per visualizzare la pagina Explorer per quell'oggetto.	Questa pagina consente di visualizzare i dettagli dell'oggetto e di confrontarlo con altri oggetti di archiviazione simili per verificare se altri oggetti di archiviazione presentano problemi di prestazioni nello stesso periodo. Ad esempio, per verificare se anche altri volumi sullo stesso aggregato presentano problemi di prestazioni.
Fare clic sul nome del cluster per visualizzare la pagina Riepilogo cluster.	Questa pagina consente di visualizzare i dettagli del cluster su cui risiede questo oggetto per verificare se si sono verificati altri problemi di prestazioni nello stesso periodo.

Analizza gli eventi dalle soglie di prestazione definite dal sistema

Gli eventi generati dalle soglie di prestazioni definite dal sistema indicano che un contatore delle prestazioni, o un set di contatori delle prestazioni, per un determinato oggetto di archiviazione ha superato la soglia di una policy definita dal sistema. Ciò indica che l'oggetto di archiviazione, ad esempio un aggregato o un nodo, sta riscontrando un problema di prestazioni.

È possibile utilizzare la pagina Dettagli evento per analizzare l'evento prestazionale e, se necessario, adottare misure correttive per riportare le prestazioni alla normalità.



I criteri di soglia definiti dal sistema non sono abilitati sui sistemi Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select .

Rispondere agli eventi di soglia delle prestazioni definiti dal sistema

È possibile utilizzare Unified Manager per analizzare gli eventi relativi alle prestazioni causati dal superamento di una soglia di avviso definita dal sistema da parte di un contatore delle prestazioni. È anche possibile utilizzare Unified Manager per verificare lo stato del componente del cluster e verificare se gli eventi recenti rilevati sul componente hanno contribuito all'evento relativo alle prestazioni.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

- Devono esserci eventi di performance nuovi o obsoleti.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Esaminare la **Descrizione**, che descrive la violazione della soglia che ha causato l'evento.

Ad esempio, il messaggio “Un valore di utilizzo del nodo del 90% ha attivato un evento di AVVISO in base all'impostazione della soglia dell'85%” indica che si è verificato un evento di avviso di utilizzo del nodo per l'oggetto cluster.

3. Prendi nota dell'**Ora di attivazione dell'evento** in modo da poter verificare se altri eventi potrebbero essersi verificati contemporaneamente e aver contribuito a questo evento.
4. In **Diagnosi di sistema**, rivedere la breve descrizione del tipo di analisi che la policy definita dal sistema sta eseguendo sull'oggetto cluster.

Per alcuni eventi, accanto alla diagnosi viene visualizzata un'icona verde o rossa per indicare se è stato rilevato un problema in quella particolare diagnosi. Per altri tipi di eventi definiti dal sistema, i grafici dei contatori mostrano le prestazioni dell'oggetto.

5. In **Azioni suggerite**, fai clic sul collegamento **Aiutami a fare questo** per visualizzare le azioni suggerite che puoi eseguire per provare a risolvere autonomamente l'evento di prestazione.

Rispondere agli eventi di prestazione del gruppo di policy QoS

Unified Manager genera eventi di avviso relativi ai criteri QoS quando la velocità effettiva del carico di lavoro (IOPS, IOPS/TB o MBps) supera l'impostazione dei criteri QoS ONTAP definiti e la latenza del carico di lavoro ne risente. Questi eventi definiti dal sistema offrono l'opportunità di correggere potenziali problemi di prestazioni prima che molti carichi di lavoro siano interessati dalla latenza.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Unified Manager genera eventi di avviso per violazioni dei criteri QoS quando la velocità effettiva del carico di lavoro ha superato l'impostazione dei criteri QoS definiti durante ogni periodo di raccolta delle prestazioni per l'ora precedente. La produttività del carico di lavoro potrebbe superare la soglia QoS solo per un breve periodo di tempo durante ogni periodo di raccolta, ma Unified Manager visualizza nel grafico solo la produttività "media" durante il periodo di raccolta. Per questo motivo potresti ricevere eventi QoS anche se la velocità effettiva di un carico di lavoro potrebbe non aver superato la soglia di policy indicata nel grafico.

È possibile utilizzare System Manager o i comandi ONTAP per gestire i gruppi di policy, incluse le seguenti attività:

- Creazione di un nuovo gruppo di policy per il carico di lavoro
- Aggiunta o rimozione di carichi di lavoro in un gruppo di policy
- Spostamento di un carico di lavoro tra gruppi di policy
- Modifica del limite di throughput di un gruppo di policy
- Spostamento di un carico di lavoro su un aggregato o nodo diverso

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Esaminare la **Descrizione**, che descrive la violazione della soglia che ha causato l'evento.

Ad esempio, il messaggio “Un valore IOPS di 1.352 IOPS su vol1_NFS1 ha attivato un evento di AVVISO per identificare potenziali problemi di prestazioni per il carico di lavoro” indica che si è verificato un evento QoS Max IOPS sul volume vol1_NFS1.

3. Consulta la sezione **Informazioni sull'evento** per vedere maggiori dettagli su quando si è verificato l'evento e per quanto tempo è stato attivo.

Inoltre, per i volumi o le LUN che condividono la velocità effettiva di una policy QoS, è possibile visualizzare i nomi dei tre carichi di lavoro principali che consumano più IOPS o MBps.

4. Nella sezione **Diagnosi di sistema**, esaminare i due grafici: uno per gli IOPS medi totali o MBps (a seconda dell'evento) e uno per la latenza. In questo modo è possibile vedere quali componenti del cluster influiscono maggiormente sulla latenza quando il carico di lavoro si avvicina al limite massimo QoS.

Per un evento di policy QoS condiviso, i tre carichi di lavoro principali vengono mostrati nel grafico della produttività. Se più di tre carichi di lavoro condividono la policy QoS, i carichi di lavoro aggiuntivi vengono aggiunti insieme nella 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 di policy QoS adattiva i grafici IOPS e MBps mostrano i valori IOPS o MBps che ONTAP ha convertito dalla policy di soglia IOPS/TB assegnata in base alle dimensioni del volume.

5. Nella sezione **Azioni suggerite**, rivedi i suggerimenti e determina quali azioni dovresti eseguire per evitare un aumento della latenza del carico di lavoro.

Se necessario, fare clic sul pulsante **Aiuto** per visualizzare maggiori dettagli sulle azioni suggerite che è possibile eseguire per provare a risolvere l'evento di prestazione.

Comprendere gli eventi provenienti da policy QoS adattive che hanno una dimensione di blocco definita

I gruppi di policy QoS adattivi ridimensionano automaticamente un limite massimo o minimo di throughput 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 nella policy QoS per applicare contemporaneamente una soglia MB/s.

L'assegnazione di una soglia IOPS in una policy QoS adattiva pone un limite solo al numero di operazioni che si verificano in ciascun carico di lavoro. A seconda della dimensione del blocco impostata sul client che genera i carichi di lavoro, alcuni IOPS includono molti più dati e quindi impongono un carico molto maggiore sui nodi che elaborano le operazioni.

Il valore MB/s per un carico di lavoro viene generato utilizzando la seguente formula:

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

Se un carico di lavoro ha una media di 3.000 IOPS e la dimensione del blocco sul client è impostata su 32 KB,

il valore effettivo di MB/s per questo carico di lavoro è 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 valore effettivo di MB/s per questo carico di lavoro è 144. È possibile notare che il nodo elabora il 50% di dati in più quando la dimensione del blocco è maggiore.

Diamo un'occhiata alla seguente policy QoS adattiva che ha una dimensione di blocco definita e al modo in cui gli eventi vengono attivati in base alla dimensione di blocco impostata sul client.

Crea una policy e imposta la velocità massima su 2.500 IOPS/TB con una dimensione del blocco di 32 KB. In questo modo la soglia MB/s viene impostata di fatto su 80 MB/s $((2500 \text{ IOPS} * 32 \text{ KB}) / 1000)$ per un volume con una capacità utilizzata di 1 TB. Si noti che Unified Manager genera un evento di avviso quando il valore della velocità effettiva è inferiore del 10% rispetto alla soglia definita. Gli eventi vengono generati nelle seguenti situazioni:

Capacità utilizzata	L'evento viene generato quando la velocità effettiva 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, gli IOPS sono 4.000 e la dimensione del blocco QoS è impostata su 32 KB sul client, la velocità effettiva MB/s è 128 MB/s $((4.000 \text{ IOPS} * 32 \text{ KB}) / 1000)$. In questo scenario non viene generato alcun evento perché sia 4.000 IOPS che 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, gli IOPS sono 4.000 e la dimensione del blocco QoS è impostata su 64 KB sul client, la velocità effettiva MB/s è 256 MB/s $((4.000 \text{ IOPS} * 64 \text{ KB}) / 1000)$. In questo caso i 4.000 IOPS non generano 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 di MB/s per una policy QoS adattiva che include la dimensione del blocco, nella sezione Diagnosi di sistema della pagina Dettagli evento viene visualizzato un grafico MB/s. Se l'evento viene attivato in base a una violazione IOPS per la policy QoS adattiva, nella sezione Diagnosi di sistema viene visualizzato un grafico IOPS. Se si verifica una violazione sia per IOPS che per MB/s, riceverai due eventi.

Per ulteriori informazioni sulla regolazione delle impostazioni QoS, vedere ["Panoramica sulla gestione delle prestazioni"](#).

Rispondere agli eventi di prestazioni di sovrautilizzo delle risorse del nodo

Unified Manager genera eventi di avviso di sovrautilizzo delle risorse del nodo quando un singolo nodo funziona oltre i limiti della sua efficienza operativa, influenzando potenzialmente le latenze del carico di lavoro. Questi eventi definiti dal sistema offrono l'opportunità di correggere potenziali problemi di prestazioni prima che molti carichi di lavoro siano interessati dalla latenza.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance nuovi o obsoleti.

Unified Manager genera eventi di avviso per violazioni delle policy di utilizzo eccessivo delle risorse dei nodi, cercando i nodi che utilizzano più del 100% della loro capacità prestazionale per più di 30 minuti.

È possibile utilizzare System Manager o i comandi ONTAP per correggere questo tipo di problema di prestazioni, incluse le seguenti attività:

- Creazione e applicazione di una policy QoS a tutti i volumi o LUN che utilizzano eccessivamente le risorse di sistema
- Riduzione del limite massimo di throughput QoS di un gruppo di policy a cui sono stati applicati carichi di lavoro
- Spostamento di un carico di lavoro su un aggregato o nodo diverso
- Aumentare la capacità aggiungendo dischi al nodo o aggiornando a un nodo con una CPU più veloce e più RAM

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Esaminare la **Descrizione**, che descrive la violazione della soglia che ha causato l'evento.

Ad esempio, il messaggio "Perf. Il valore di Capacità utilizzata del 139% su simplicity-02 ha attivato un evento di AVVISO per identificare potenziali problemi di prestazioni nell'unità di elaborazione dati." indica che la capacità di prestazioni sul nodo simplicity-02 è sovrautilizzata e influisce sulle prestazioni del nodo.

3. Nella sezione **Diagnosi di sistema**, esaminare i tre grafici: uno per la capacità di prestazioni 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. Organizzandoli in questo modo è possibile vedere quali carichi di lavoro sono la causa della latenza sul nodo.

È possibile visualizzare a quali carichi di lavoro sono applicati criteri QoS e a quali no, spostando il cursore sul grafico IOPS.

4. Nella sezione **Azioni suggerite**, rivedi i suggerimenti e determina quali azioni dovresti eseguire per evitare un aumento della latenza del carico di lavoro.

Se necessario, fare clic sul pulsante **Aiuto** per visualizzare maggiori dettagli sulle azioni suggerite che è possibile eseguire per provare a risolvere l'evento di prestazione.

Rispondere agli eventi di prestazioni di squilibrio del cluster

Unified Manager genera eventi di avviso di squilibrio del cluster quando un nodo in un cluster opera con un carico molto più elevato rispetto agli altri nodi, influenzando potenzialmente le latenze del carico di lavoro. Questi eventi definiti dal sistema offrono l'opportunità di correggere potenziali problemi di prestazioni prima che molti carichi di lavoro siano interessati dalla latenza.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Unified Manager genera eventi di avviso per le violazioni della policy di soglia di squilibrio del cluster confrontando il valore della capacità prestazionale utilizzata per tutti i nodi del cluster per verificare se esiste una differenza di carico del 30% tra i nodi.

Questi passaggi ti aiutano a identificare le seguenti risorse in modo da poter spostare carichi di lavoro ad alte prestazioni su un nodo meno utilizzato:

- I nodi sullo stesso cluster che sono meno utilizzati
- Gli aggregati sul nuovo nodo che sono meno utilizzati
- I volumi più performanti sul nodo corrente

Passi

1. Visualizza la pagina dei dettagli dell'**Evento** per visualizzare le informazioni sull'evento.
2. Esaminare la **Descrizione**, che descrive la violazione della soglia che ha causato l'evento.

Ad esempio, il messaggio "Il contatore della capacità di prestazione utilizzata indica una differenza di carico del 62% tra i nodi sul cluster Dallas-1-8 e ha attivato un evento di AVVISO in base alla soglia di sistema del 30%" indica che la capacità di prestazione su uno dei nodi è sovrautilizzata e influisce sulle prestazioni del nodo.

3. Esaminare il testo nelle **Azioni suggerite** per spostare un volume ad alte prestazioni dal nodo con il valore di capacità ad alte prestazioni utilizzato a un nodo con il valore di capacità a prestazioni più basso utilizzato.
4. Identificare i nodi con il valore di capacità di prestazioni utilizzato più alto e più basso:
 - a. Nella sezione **Informazioni sull'evento**, fare clic sul nome del cluster di origine.
 - b. Nella pagina **Riepilogo cluster/prestazioni**, fare clic su **Nodi** nell'area **Oggetti gestiti**.
 - c. Nella pagina dell'inventario **Nodi**, ordina i nodi in base alla colonna **Capacità di prestazioni utilizzata**.
 - d. Identificare i nodi con il valore di capacità di prestazioni più alto e più basso utilizzato e annotarne i nomi.
5. Identifica il volume che utilizza il maggior numero di IOPS sul nodo che ha il valore di capacità di prestazioni utilizzato più elevato:
 - a. Fare clic sul nodo con il valore di capacità di prestazioni utilizzato più elevato.
 - b. Nella pagina **Esplora nodi/prestazioni**, seleziona **Aggregati su questo nodo** dal menu **Visualizza e confronta**.
 - c. Fare clic sull'aggregato con il valore di capacità di prestazioni utilizzato più elevato.
 - d. Nella pagina **Aggregate / Performance Explorer**, seleziona **Volumi su questo aggregato** dal menu **Visualizza e confronta**.
 - e. Ordinare i volumi in base alla colonna **IOPS** e annotare il nome del volume che utilizza il maggior numero di IOPS e il nome dell'aggregato in cui risiede il volume.
6. Identificare l'aggregato con il minor utilizzo sul nodo che ha il valore di capacità di prestazioni utilizzato più basso:
 - a. Fare clic su **Archiviazione > Aggregati** per visualizzare la pagina dell'inventario **Aggregati**.
 - b. Selezionare la vista **Prestazioni: Tutti gli aggregati**.
 - c. Fare clic sul pulsante **Filtro** e aggiungere un filtro in cui "Nodo" è uguale al nome del nodo con il valore di capacità di prestazioni utilizzato più basso annotato nel passaggio 4.

- d. Annotare il nome dell'aggregato che ha il valore di capacità prestazionale utilizzato più basso.
7. Spostare il volume dal nodo sovraccarico all'aggregato identificato come poco utilizzato sul nuovo nodo.

È possibile eseguire l'operazione di spostamento utilizzando ONTAP System Manager, OnCommand Workflow Automation, i comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, controlla se stai ricevendo lo stesso evento di squilibrio del cluster da questo cluster.

Analizza gli eventi dalle soglie di prestazioni 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. È possibile utilizzare la pagina Dettagli evento per analizzare l'evento prestazionale e, se necessario, adottare misure correttive per riportare le prestazioni alla normalità.



Le soglie di prestazioni dinamiche non sono abilitate sui sistemi Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select.

Identificare i carichi di lavoro delle vittime coinvolti in un evento di prestazioni dinamiche

In Unified Manager è possibile identificare quali carichi di lavoro di volume presentano la deviazione più elevata nel tempo di risposta (latenza) causata da un componente di archiviazione in contesa. Identificare questi carichi di lavoro aiuta a capire perché le applicazioni client che vi accedono sono più lente del solito.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance dinamica 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 maggiormente interessati dall'evento. I valori si basano sui picchi identificati da Unified Manager quando ha rilevato e analizzato per l'ultima volta l'evento.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Nei grafici Latenza del carico di lavoro e Attività del carico di lavoro, selezionare **Carichi di lavoro delle vittime**.
3. Passa il cursore sui grafici per visualizzare i principali carichi di lavoro definiti dall'utente che interessano il componente e il nome del carico di lavoro interessato.

Identificare i carichi di lavoro eccessivi coinvolti in un evento di performance dinamica

In Unified Manager è possibile identificare quali carichi di lavoro presentano la deviazione più elevata nell'utilizzo per un componente del cluster in competizione. L'identificazione di questi carichi di lavoro aiuta a comprendere perché determinati volumi del cluster

presentano tempi di risposta lenti (latenza).

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance dinamica nuovi, riconosciuti o obsoleti.

La pagina Dettagli evento visualizza un elenco dei carichi di lavoro definiti dall'utente e dal sistema, classificati in base al maggiore utilizzo del componente o al maggiore impatto dell'evento. I valori si basano sui picchi identificati da Unified Manager quando ha rilevato e analizzato per l'ultima volta l'evento.

Passi

1. Visualizza la pagina Dettagli evento per visualizzare le informazioni sull'evento.
2. Nei grafici Latenza del carico di lavoro e Attività del carico di lavoro, seleziona **Carichi di lavoro pesanti**.
3. Passa il cursore sui grafici per visualizzare i principali carichi di lavoro definiti dall'utente che influiscono sul componente.

Identificare i carichi di lavoro degli squali coinvolti in un evento di performance dinamica

In Unified Manager è possibile identificare quali carichi di lavoro presentano la deviazione più elevata nell'utilizzo per un componente di archiviazione in competizione. L'identificazione di questi carichi di lavoro aiuta a stabilire se è opportuno spostarli in un cluster meno utilizzato.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Ci sono eventi dinamici di performance nuovi, riconosciuti o obsoleti.

La pagina Dettagli evento visualizza un elenco dei carichi di lavoro definiti dall'utente e dal sistema, classificati in base al maggiore utilizzo del componente o al maggiore impatto dell'evento. I valori si basano sui picchi identificati da Unified Manager quando ha rilevato e analizzato per l'ultima volta l'evento.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Nei grafici Latenza del carico di lavoro e Attività del carico di lavoro, seleziona **Carichi di lavoro Shark**.
3. Passa 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 Shark.

Analisi degli eventi prestazionali per una configurazione MetroCluster

È possibile utilizzare Unified Manager per analizzare un evento di prestazioni 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 prestazioni MetroCluster potrebbero essere dovuti a carichi di lavoro eccessivi che sfruttano eccessivamente i collegamenti interswitch (ISL) tra i cluster oppure a problemi di integrità dei collegamenti. Unified Manager monitora ogni cluster in una configurazione MetroCluster in modo indipendente, senza considerare gli eventi relativi alle prestazioni su un cluster partner.

Gli eventi relativi alle prestazioni di entrambi i cluster nella configurazione MetroCluster vengono visualizzati anche nella pagina Dashboard di Unified Manager. È anche possibile visualizzare le pagine Integrità di Unified Manager per controllare lo stato di ciascun cluster e visualizzarne le relazioni.

Analizza un evento di prestazioni dinamiche 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 prestazioni. È possibile identificare il nome del cluster, l'ora di rilevamento dell'evento e i carichi di lavoro *bullo* e *vittima* coinvolti.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Per una configurazione MetroCluster devono essere presenti eventi di prestazione nuovi, riconosciuti o obsoleti.
- Entrambi i cluster nella configurazione MetroCluster devono essere monitorati dalla stessa istanza di Unified Manager.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Esaminare la descrizione dell'evento per vedere i nomi dei carichi di lavoro coinvolti e il loro numero.

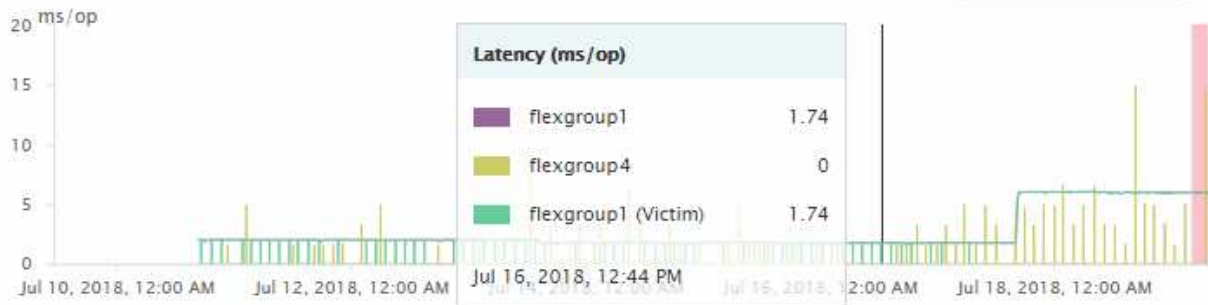
In questo esempio, l'icona Risorse MetroCluster è rossa, a indicare che le risorse MetroCluster sono in competizione. Posiziona il cursore sull'icona per visualizzarne la descrizione.



3. Prendi nota del nome del cluster e dell'ora di rilevamento dell'evento, che puoi utilizzare per analizzare gli eventi relativi alle prestazioni sul cluster partner.
4. Nei grafici, esamina i carichi di lavoro delle *vittime* per confermare che i loro tempi di risposta siano superiori alla soglia di prestazione.

In questo esempio, il carico di lavoro della vittima viene visualizzato nel testo in evidenza. 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 della vittima ha attivato l'evento, un modello di latenza coerente potrebbe indicare che i carichi di lavoro stanno funzionando entro l'intervallo previsto, ma che un picco di I/O ha aumentato la latenza e attivato l'evento.

Workload Latency



Se di recente hai installato un'applicazione su un client che accede a questi carichi di lavoro 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 cambia in obsoleto e rimane in questo stato per più di 30 minuti, probabilmente puoi ignorare l'evento. Se l'evento è in corso e rimane nel nuovo stato, puoi indagare ulteriormente per determinare se altri problemi lo hanno causato.

5. Nel grafico Capacità di elaborazione del carico di lavoro, selezionare **Carichi di lavoro in eccesso** per visualizzare i carichi di lavoro in eccesso.

La presenza di carichi di lavoro eccessivi indica che l'evento potrebbe essere stato causato da uno o più carichi di lavoro sul cluster locale che hanno utilizzato eccessivamente le risorse MetroCluster. I carichi di lavoro più pesanti presentano un'elevata deviazione nella velocità di scrittura (MB/s).

Questo grafico mostra, ad alto livello, il modello di velocità di scrittura (MB/s) per i carichi di lavoro. È possibile esaminare il modello MB/s di scrittura per identificare una velocità effettiva anomala, che potrebbe indicare che un carico di lavoro sta utilizzando eccessivamente le risorse MetroCluster.

Se nell'evento non sono coinvolti carichi di lavoro indesiderati, l'evento potrebbe essere stato causato da un problema di integrità del collegamento tra i cluster o da un problema di prestazioni sul cluster partner. È possibile utilizzare Unified Manager per verificare lo stato di entrambi i cluster in una configurazione MetroCluster. È anche possibile utilizzare Unified Manager per verificare e analizzare gli eventi relativi alle prestazioni nel cluster partner.

Analizza un evento di prestazioni dinamiche per un cluster remoto su una configurazione MetroCluster

È possibile utilizzare Unified Manager per analizzare gli eventi di prestazioni dinamiche su un cluster remoto in una configurazione MetroCluster. L'analisi consente di determinare se un evento sul cluster remoto ha causato un evento sul cluster partner.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver analizzato un evento di prestazioni su un cluster locale in una configurazione MetroCluster e ottenuto il tempo di rilevamento dell'evento.
- È necessario aver verificato lo stato del cluster locale e del cluster partner coinvolto nell'evento di prestazione e aver ottenuto il nome del cluster partner.

Passi

1. Accedi all'istanza di Unified Manager che monitora il cluster partner.
2. Nel riquadro di navigazione a sinistra, fare clic su **Eventi** per visualizzare l'elenco degli eventi.
3. Dal selettore **Intervallo di tempo**, seleziona **Ultima ora**, quindi fai clic su **Applica intervallo**.
4. Nel selettore **Filtro**, seleziona **Cluster** dal menu a discesa a sinistra, digita il nome del cluster partner nel campo di testo, quindi fai clic su **Applica filtro**.

Se non si sono verificati eventi per il cluster selezionato nell'ultima ora, ciò indica che il cluster non ha riscontrato problemi di prestazioni durante il periodo in cui l'evento è stato rilevato sul suo partner.

5. Se nel cluster selezionato sono stati rilevati eventi nell'ultima ora, confrontare l'ora di rilevamento dell'evento con l'ora di rilevamento dell'evento per l'evento nel cluster locale.

Se questi eventi comportano carichi di lavoro eccessivi che causano conflitti sul componente di elaborazione dati, uno o più di questi carichi eccessivi potrebbero aver causato l'evento sul cluster locale. Puoi cliccare sull'evento per analizzarlo e rivedere le azioni suggerite per risolverlo nella pagina dei dettagli dell'evento.

Se questi eventi non comportano carichi di lavoro eccessivi, non hanno causato l'evento di prestazioni sul cluster locale.

Rispondere a un evento di prestazioni dinamiche causato dalla limitazione del gruppo di criteri QoS

È possibile utilizzare Unified Manager per analizzare un evento di prestazioni causato da un gruppo di policy di qualità del servizio (QoS) che limita la velocità effettiva del carico di lavoro (MB/s). La limitazione ha aumentato i tempi di risposta (latenza) dei carichi di lavoro di volume nel gruppo di policy. È possibile utilizzare le informazioni sull'evento per determinare se sono necessari nuovi limiti sui gruppi di policy per interrompere la limitazione.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Leggere la **Descrizione**, che mostra il nome dei carichi di lavoro interessati dalla limitazione.



La descrizione può mostrare lo stesso carico di lavoro per la vittima e per il bullo, perché la limitazione rende il carico di lavoro 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 seguito.

4. Nei grafici Latenza del carico di lavoro e Utilizzo del carico di lavoro, seleziona **Carichi di lavoro pesanti**.
5. Passa il cursore sui grafici per visualizzare i principali carichi di lavoro definiti dall'utente che incidono sul gruppo di policy.

Il carico di lavoro in cima all'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 suggerite**, fare clic sul pulsante **Analizza carico di lavoro** per il carico di lavoro principale.
7. Nella pagina Analisi del carico di lavoro, imposta il grafico Latenza per visualizzare tutti i componenti del cluster e il grafico Throughput per visualizzare la ripartizione.

I grafici di ripartizione vengono visualizzati sotto il grafico Latenza e il grafico IOPS.

8. Confronta i limiti QoS nel grafico **Latenza** per vedere quale livello di limitazione ha influito sulla latenza al momento dell'evento.

Il gruppo di policy QoS ha una capacità massima di 1.000 operazioni al secondo (op/sec), che i carichi di lavoro al suo interno non possono superare collettivamente. Al momento dell'evento, i carichi di lavoro nel gruppo di policy avevano una capacità effettiva combinata di oltre 1.200 operazioni/sec, il che ha costretto il gruppo di policy a ridurre la propria attività a 1.000 operazioni/sec.

9. Confronta i valori di **Latenza di lettura/scrittura** con i valori di **Letture/scritture/altro**.

Entrambi i grafici mostrano un numero elevato di richieste di lettura con elevata latenza, ma il numero di richieste e la quantità di latenza per le richieste di scrittura sono bassi. Questi valori aiutano a determinare se è presente un'elevata quantità di throughput o un numero elevato di operazioni che hanno aumentato la latenza. È possibile utilizzare questi valori quando si decide di impostare un limite di gruppo di policy sulla velocità effettiva o sulle operazioni.

10. Utilizzare ONTAP System Manager per aumentare il limite corrente sul gruppo di policy a 1.300 operazioni/sec.
11. Dopo un giorno, torna a Unified Manager e inserisci il carico di lavoro registrato nel passaggio 3 nella pagina **Analisi del carico di lavoro**.
12. Selezionare il grafico Ripartizione della produttività.

Viene visualizzato il grafico Letture/scritture/altro.

13. Nella parte superiore della pagina, punta il cursore sull'icona dell'evento di modifica () per la modifica del limite del gruppo di policy.
14. Confronta il grafico **Letture/scritture/altro** con il grafico **Latenza**.

Le richieste di lettura e scrittura sono le stesse, ma la limitazione è stata interrotta e la latenza è diminuita.

Rispondere a un evento di prestazioni dinamiche causato da un guasto del disco

È possibile utilizzare Unified Manager per analizzare un evento di prestazioni causato da carichi di lavoro che utilizzano eccessivamente un aggregato. È anche possibile utilizzare Unified Manager per verificare lo stato di integrità dell'aggregato e verificare se gli eventi di integrità recenti rilevati sull'aggregato hanno contribuito all'evento di prestazioni.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Leggere la **Descrizione**, che descrive i carichi di lavoro coinvolti nell'evento e il componente del cluster in competizione.

Sono presenti più volumi vittima la cui latenza è stata influenzata dal componente cluster in conflitto. L'aggregato, che si trova nel mezzo di una ricostruzione RAID per sostituire il disco guasto con un disco di riserva, è il componente del cluster in competizione. In Componente in contesa, l'icona Aggregato è evidenziata in rosso e il nome dell'aggregato è visualizzato tra parentesi.

3. Nel grafico Utilizzo del carico di lavoro, seleziona **Carichi di lavoro pesanti**.
4. Passa il cursore sul grafico per visualizzare i carichi di lavoro più intensi che incidono sul componente.

Nella parte superiore del grafico vengono visualizzati i carichi di lavoro principali con il picco di utilizzo più elevato da quando è stato rilevato l'evento. Uno dei carichi di lavoro principali è il carico di lavoro Disk Health definito dal sistema, che indica una ricostruzione RAID. La ricostruzione è il processo interno che consiste nel ricostruire l'aggregato con il disco di riserva. Il carico di lavoro Disk Health, insieme ad altri carichi di lavoro sull'aggregato, ha probabilmente causato il conflitto sull'aggregato e l'evento associato.

5. Dopo aver confermato che l'attività del carico di lavoro Disk Health ha causato l'evento, attendere circa 30 minuti affinché la ricostruzione venga completata e Unified Manager analizzi l'evento e rilevi se l'aggregato è ancora in conflitto.
6. Aggiorna i **Dettagli dell'evento**.

Una volta completata la ricostruzione del RAID, verificare che lo Stato sia obsoleto, a indicare che l'evento è stato risolto.

7. Nel grafico Utilizzo del carico di lavoro, selezionare **Carichi di lavoro elevati** per visualizzare i carichi di lavoro aggregati in base al picco di utilizzo.
8. Nell'area **Azioni suggerite**, fare clic sul pulsante **Analizza carico di lavoro** per il carico di lavoro principale.
9. Nella pagina **Analisi del carico di lavoro**, impostare l'intervallo di tempo per visualizzare le ultime 24 ore (1 giorno) di dati per il volume selezionato.

Nella cronologia degli eventi, un punto rosso (●) indica quando si è verificato l'evento di errore del disco.

10. Nel grafico Utilizzo nodi e aggregati, nascondere la linea per le statistiche dei nodi in modo che rimanga solo la linea Aggregata.
11. Confronta i dati in questo grafico con i dati al momento dell'evento nel grafico **Latenza**.

Al momento dell'evento, l'Utilizzo 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 l'evento, sia le letture che le scritture e la latenza sono diminuite, confermando che l'aggregato non è più in competizione.

Rispondere a un evento di prestazioni dinamiche causato dall'acquisizione di HA

È possibile utilizzare Unified Manager per analizzare un evento di prestazioni causato da un'elaborazione dati elevata su un nodo del cluster che si trova in una coppia ad alta disponibilità (HA). È anche possibile utilizzare Unified Manager per verificare lo stato di integrità dei nodi e verificare se eventuali eventi di integrità rilevati di recente sui nodi

hanno contribuito all'evento di prestazioni.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Passi

1. Visualizza la pagina **Dettagli evento** per visualizzare le informazioni sull'evento.
2. Leggere la **Descrizione**, che descrive i carichi di lavoro coinvolti nell'evento e il componente del cluster in competizione.

Esiste un volume vittima la cui latenza è stata influenzata dal componente cluster in conflitto. Il nodo di elaborazione dati, che ha preso in carico tutti i carichi di lavoro dal suo nodo partner, è il componente del cluster in competizione. In Componente in conflitto, l'icona Data Processing è evidenziata in rosso e il nome del nodo che gestiva l'elaborazione dati al momento dell'evento è visualizzato tra parentesi.

3. Nella **Descrizione**, fare clic sul nome del volume.

Viene visualizzata la pagina Volume Performance Explorer. Nella parte superiore della pagina, nella cronologia degli eventi, un'icona di modifica dell'evento () indica l'ora in cui Unified Manager ha rilevato l'inizio del takeover HA.

4. Posiziona il cursore sull'icona dell'evento di modifica per l'acquisizione HA e i dettagli sull'acquisizione HA verranno visualizzati nel testo passante.

Nel grafico Latenza, un evento indica che il volume selezionato ha superato la soglia di prestazioni a causa dell'elevata latenza più o meno nello stesso momento dell'acquisizione HA.

5. Fare clic su **Zoom vista** per visualizzare il grafico della latenza in una nuova pagina.
6. Nel menu Visualizza, seleziona **Componenti del cluster** per visualizzare la latenza totale per componente del cluster.
7. Punta il cursore del mouse sull'icona dell'evento di modifica per l'avvio dell'acquisizione HA e confronta la latenza per l'elaborazione dei dati con la latenza totale.

Al momento dell'acquisizione di HA, si è verificato un picco nell'elaborazione dei dati dovuto all'aumento del carico di lavoro richiesto sul nodo di elaborazione dati. L'aumento dell'utilizzo della CPU ha aumentato la latenza e ha attivato l'evento.

8. Dopo aver riparato il nodo guasto, utilizzare ONTAP System Manager per eseguire un giveback HA, che sposta i carichi di lavoro dal nodo partner al nodo riparato.
9. Una volta completato il giveback HA, dopo la successiva individuazione della configurazione in Unified Manager (circa 15 minuti), individuare l'evento e il carico di lavoro attivati dal takeover HA nella pagina dell'inventario **Gestione eventi**.

L'evento attivato dall'acquisizione HA ha ora uno stato obsoleto, che indica che l'evento è stato risolto. La latenza nel componente di elaborazione dei dati è diminuita, con conseguente diminuzione della latenza totale. Il nodo che il volume selezionato sta utilizzando per l'elaborazione dei dati ha risolto l'evento.

Risolvere gli eventi di performance

È possibile utilizzare le azioni suggerite per provare a risolvere autonomamente gli eventi relativi alle prestazioni. I primi tre suggerimenti vengono sempre visualizzati, mentre le azioni previste dal quarto suggerimento sono specifiche del tipo di evento visualizzato.

I link **Aiutami a fare questo** forniscono informazioni aggiuntive per ogni azione suggerita, comprese le istruzioni per eseguire un'azione specifica. Alcune azioni potrebbero comportare l'utilizzo di Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, comandi ONTAP CLI o una combinazione di questi strumenti.

Verificare che la latenza sia compresa nell'intervallo previsto

Quando un componente del cluster è in competizione, i carichi di lavoro del volume che lo utilizzano potrebbero avere tempi di risposta (latenza) ridotti. È possibile esaminare la latenza di ciascun carico di lavoro della vittima sul componente in conflitto per confermare che la latenza effettiva rientri nell'intervallo previsto. È anche possibile fare clic sul nome di un volume per visualizzarne i dati storici.

Se l'evento di performance si trova nello stato obsoleto, la latenza di ciascuna vittima coinvolta nell'evento potrebbe essere rientrata nell'intervallo previsto.

Esaminare l'impatto delle modifiche alla configurazione sulle prestazioni del carico di lavoro

Le modifiche alla configurazione del cluster, come un disco guasto, un failover HA o uno spostamento di volume, potrebbero avere un impatto negativo sulle prestazioni 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 alla 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 prestazioni di Unified Manager possono rilevare solo un numero limitato di eventi di modifica. Le pagine relative allo stato di salute forniscono avvisi per altri eventi causati da modifiche alla configurazione. È possibile cercare il volume in Unified Manager per visualizzare la cronologia degli eventi.

Opzioni per migliorare le prestazioni del carico di lavoro dal lato client

È possibile controllare i carichi di lavoro dei client, come applicazioni o database, che inviano I/O ai volumi coinvolti in un evento di prestazioni per determinare se una modifica sul lato client potrebbe correggere l'evento.

Quando i client connessi ai volumi di un cluster aumentano le loro richieste di I/O, il cluster deve lavorare di più per soddisfare la domanda. Se si sa quali client hanno un numero elevato di richieste di I/O su un particolare volume del cluster, è possibile migliorare le prestazioni del cluster regolando il numero di client che accedono al volume o riducendo la quantità di I/O sul volume. È anche possibile applicare o aumentare un limite al gruppo di policy QoS di cui il volume è membro.

È possibile analizzare i client e le relative applicazioni per determinare se i client inviano più I/O del solito, il

che potrebbe causare conflitti su un componente del cluster. Nella pagina Dettagli evento, la sezione Diagnosi di sistema visualizza i carichi di lavoro del volume principale che utilizzano il componente in competizione. Se si sa quale client sta accedendo a un volume specifico, è possibile andare al client per determinare se l'hardware del client o un'applicazione non funziona come previsto o sta eseguendo più lavoro del solito.

In una configurazione MetroCluster, le richieste di scrittura su un volume su un cluster locale vengono replicate su un volume sul cluster remoto. Mantenere sincronizzato il volume di origine sul cluster locale con il volume di destinazione sul cluster remoto può anche aumentare la richiesta di entrambi i cluster nella configurazione MetroCluster. Riducendo le richieste di scrittura su questi volumi mirror, i cluster possono eseguire meno operazioni di sincronizzazione, riducendo così l'impatto sulle prestazioni di altri carichi di lavoro.

Verificare la presenza di problemi con il client o con la rete

Quando i client connessi ai volumi di un cluster aumentano le loro richieste di I/O, il cluster deve lavorare di più per soddisfare la domanda. L'aumento della domanda sul cluster può mettere in competizione un componente, aumentare la latenza dei carichi di lavoro che lo utilizzano e attivare un evento in Unified Manager.

Nella pagina Dettagli evento, la sezione Diagnosi di sistema visualizza i carichi di lavoro del volume principale che utilizzano il componente in competizione. Se si sa quale client sta accedendo a un volume specifico, è possibile andare al client per determinare se l'hardware del client o un'applicazione non funziona come previsto o sta eseguendo 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 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 presentano un'attività insolitamente elevata

È possibile esaminare i carichi di lavoro nel gruppo di policy Qualità del servizio (QoS) con la variazione più elevata nell'attività per determinare se l'evento è stato causato da più di un carico di lavoro. È anche possibile verificare se altri carichi di lavoro superano ancora il limite di produttività impostato o se rientrano nell'intervallo di attività previsto.

Nella pagina Dettagli evento, nella sezione Diagnosi di sistema, è possibile ordinare i carichi di lavoro in base alla deviazione massima dell'attività per visualizzare i carichi di lavoro con la variazione di attività più elevata nella parte superiore della tabella. Questi carichi di lavoro potrebbero essere i "bulli" la cui attività ha superato il limite stabilito e potrebbe aver causato l'evento.

È possibile accedere alla pagina Analisi del carico di lavoro per ciascun carico di lavoro del volume per esaminare l'attività IOPS. Se il carico di lavoro prevede periodi di attività operativa molto intensa, potrebbe aver contribuito all'evento. È possibile modificare le impostazioni del gruppo di policy per il carico di lavoro o spostare il carico di lavoro in un gruppo di policy diverso.

È possibile utilizzare ONTAP System Manager o i comandi ONTAP CLI per gestire i gruppi di policy, come segue:

- Creare un gruppo di policy.
- 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 policy.

Spostare le interfacce logiche (LIF)

Spostare le interfacce logiche (LIF) su una porta meno trafficata può aiutare a migliorare il bilanciamento del carico, agevolare le operazioni di manutenzione e l'ottimizzazione delle prestazioni e ridurre l'accesso indiretto.

L'accesso indiretto può ridurre l'efficienza del sistema. Si verifica quando un carico di lavoro di volume utilizza nodi diversi per l'elaborazione di rete e l'elaborazione dei dati. Per ridurre l'accesso indiretto, è possibile riorganizzare i LIF, ovvero spostarli in modo che utilizzino lo stesso nodo per l'elaborazione di rete e l'elaborazione dei dati. È possibile configurare il bilanciamento del carico in modo che ONTAP sposti automaticamente i LIF occupati su una porta diversa oppure è possibile spostare un LIF manualmente.

Benefici	Considerazioni
• Migliorare il bilanciamento del carico. • Ridurre l'accesso indiretto.	 Quando si sposta un LIF connesso alle condivisioni CIFS, i client che accedono alle condivisioni CIFS vengono disconnessi. Tutte le richieste di lettura o scrittura sulle condivisioni CIFS vengono interrotte.

Per configurare il bilanciamento del carico si utilizzano i comandi ONTAP . Per ulteriori informazioni, consultare la documentazione sulla rete ONTAP .

Per spostare manualmente i LIF, utilizzare ONTAP System Manager e i comandi ONTAP CLI.

Eseguire operazioni di efficienza di archiviazione in orari meno impegnativi

È possibile modificare la policy o la pianificazione che gestisce le operazioni di efficienza dell'archiviazione in modo che vengano eseguite quando i carichi di lavoro del volume interessato sono meno impegnati.

Le operazioni di efficienza dell'archiviazione possono utilizzare una quantità elevata di risorse della CPU del cluster e diventare un ostacolo per i volumi su cui vengono eseguite le operazioni. Se i volumi delle vittime presentano un'attività elevata nello stesso momento in cui vengono eseguite le operazioni di efficienza dello storage, la loro latenza può aumentare e innescare un evento.

Nella pagina Dettagli evento, la sezione Diagnosi di sistema visualizza i carichi di lavoro nel gruppo di policy QoS in base alla deviazione massima nell'attività per identificare i carichi di lavoro più problematici. Se nella parte superiore della tabella viene visualizzata la dicitura ``efficienza di archiviazione', queste operazioni stanno sovraccaricando i carichi di lavoro della vittima. Modificando la politica di efficienza o la pianificazione in modo che vengano eseguite quando questi carichi di lavoro sono meno impegnati, è possibile impedire che le operazioni di efficienza dello storage causino conflitti su un cluster.

È possibile utilizzare ONTAP System Manager per gestire le policy di efficienza. È possibile utilizzare i comandi ONTAP per gestire politiche e pianificazioni di efficienza.

Cos'è l'efficienza di archiviazione

L'efficienza di archiviazione consente di archiviare la massima quantità di dati al costo più basso e di gestire la rapida crescita dei dati, consumando meno spazio. La strategia NetApp per l'efficienza dello storage si basa sulle fondamenta integrate della virtualizzazione dello storage e dello storage unificato fornite dal suo sistema operativo ONTAP e dal file system Write Anywhere File Layout (WAFL).

L'efficienza di archiviazione include l'utilizzo di tecnologie quali thin provisioning, copia Snapshot, deduplicazione, compressione dati, FlexClone, thin replication con SnapVault e volume SnapMirror, RAID-DP, Flash Cache, Flash Pool aggregate e aggregati abilitati FabricPool che contribuiscono ad aumentare l'utilizzo dell'archiviazione e a ridurre i costi.

L'architettura di storage unificata consente di consolidare in modo efficiente una rete di archiviazione (SAN), un sistema di storage collegato alla rete (NAS) e uno storage secondario su un'unica piattaforma.

Le unità disco ad alta densità, come le unità SATA (Serial Advanced Technology Attachment) configurate nell'aggregato Flash Pool o con tecnologia Flash Cache e RAID-DP, aumentano l'efficienza senza compromettere le prestazioni e la resilienza.

Un aggregato abilitato per FabricPool include un aggregato completamente SSD o un aggregato HDD (a partire da ONTAP 9.8) come livello di prestazioni locale e un archivio oggetti specificato come livello cloud. La configurazione FabricPool consente di gestire il livello di archiviazione (locale o cloud) in cui archiviare i dati, in base alla frequenza di accesso ai dati.

Tecnologie quali thin provisioning, Snapshot copy, deduplicazione, compressione dati, thin replication con SnapVault e volume SnapMirror e FlexClone offrono maggiori risparmi. È possibile utilizzare queste tecnologie singolarmente o insieme per ottenere la massima efficienza di archiviazione.

Aggiungi dischi e rialloca i dati

È possibile aggiungere dischi a un aggregato per aumentarne la capacità di archiviazione e le prestazioni. Dopo aver aggiunto i dischi, noterai un miglioramento nelle 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 prestazioni definite dal sistema:

- Quando si riceve un evento di soglia dinamica, nella pagina Dettagli evento, l'icona del componente cluster che rappresenta l'aggregato in competizione è evidenziata in rosso.

Sotto l'icona, tra parentesi, è riportato il nome dell'aggregato, che identifica l'aggregato a cui è possibile aggiungere dischi.

- Quando si riceve un evento soglia definito dal sistema, nella pagina Dettagli evento, il testo della descrizione dell'evento elenca il nome dell'aggregato che presenta 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 acquistarne altri. È possibile utilizzare ONTAP System Manager 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 sugli aggregati SSD o FabricPool.

Come l'abilitazione della Flash Cache su un nodo può migliorare le prestazioni del carico di lavoro

È possibile migliorare le prestazioni del carico di lavoro abilitando la memorizzazione intelligente dei dati nella cache Flash Cache™ su ciascun nodo del cluster.

Un modulo Flash Cache, o modulo di memoria basato su PCIe Performance Acceleration Module, ottimizza le prestazioni dei carichi di lavoro ad alta intensità di lettura casuale, funzionando come una cache di lettura esterna intelligente. Questo hardware funziona in tandem con il componente software WAFL External Cache di ONTAP.

In Unified Manager, nella pagina Dettagli evento, l'icona del componente cluster che rappresenta l'aggregato in competizione è evidenziata in rosso. Sotto l'icona, tra parentesi, è riportato il nome dell'aggregato, che lo identifica. È possibile abilitare Flash Cache sul nodo su cui risiede l'aggregato.

È possibile utilizzare ONTAP System Manager o i comandi ONTAP per verificare se Flash Cache è installato o abilitato e per abilitarlo se non è già abilitato. Il seguente comando indica se Flash Cache è abilitato su un nodo specifico: **cluster::> run local options flexscale.enable**

Per ulteriori informazioni su Flash Cache e sui requisiti per il suo utilizzo, consultare il seguente report tecnico:

["Rapporto tecnico 3832: Guida alle best practice per la cache flash"](#)

Come l'abilitazione di Flash Pool su un aggregato di storage può migliorare le prestazioni del carico di lavoro

È possibile migliorare le prestazioni del carico di lavoro abilitando la funzionalità Flash Pool su un aggregato. Un Flash Pool è un aggregato che incorpora sia HDD che SSD. Gli HDD vengono utilizzati per l'archiviazione primaria, mentre gli SSD forniscono una cache di lettura e scrittura ad alte prestazioni per aumentare le prestazioni aggregate.

In Unified Manager, la pagina Dettagli evento visualizza il nome dell'aggregato in competizione. È possibile utilizzare ONTAP System Manager o i comandi ONTAP per verificare se Flash Pool è abilitato per un aggregato. Se hai installato degli SSD, puoi utilizzare l'interfaccia della riga di comando per abilitarli. Se hai installato degli SSD, puoi eseguire il seguente comando sull'aggregato per verificare se Flash Pool è abilitato: **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 questione.

Per ulteriori informazioni su Flash Pool e sui requisiti per il suo utilizzo, consultare la [Guida alla gestione dello storage fisico di Clustered Data ONTAP](#).

Controllo dello stato di integrità della configurazione MetroCluster

È possibile utilizzare Unified Manager per verificare lo stato dei cluster in una configurazione MetroCluster tramite IP o FC. Lo stato di integrità e gli eventi ti aiutano a determinare se ci sono problemi hardware o software che potrebbero influire sulle prestazioni dei tuoi carichi di lavoro.

Se configuri Unified Manager per l'invio di avvisi tramite e-mail, puoi controllare la tua posta elettronica per individuare eventuali problemi di integrità sul cluster locale o remoto che potrebbero aver contribuito a un evento di prestazioni. Nell'interfaccia utente grafica di Unified Manager, è possibile selezionare **Gestione eventi** per visualizzare un elenco degli eventi correnti e quindi utilizzare i filtri per visualizzare solo gli eventi di configurazione MetroCluster .

Per maggiori informazioni, vedere ["Controllo dello stato di integrità dei cluster in una configurazione MetroCluster"](#)

Verifica della configurazione MetroCluster

È possibile prevenire problemi di prestazioni per carichi di lavoro speculari in un MetroCluster su configurazioni FC e IP assicurandosi che la configurazione MetroCluster sia impostata correttamente. È anche possibile migliorare le prestazioni del carico di lavoro modificando la configurazione o aggiornando i componenti software o hardware.

Fare riferimento a ["Documentazione MetroCluster"](#) per le istruzioni su come impostare i cluster nella configurazione MetroCluster , inclusi gli switch Fibre Channel (FC), i cavi e i collegamenti inter-switch (ISL). Aiuta inoltre a 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 su IP, vedere ["Installa una configurazione IP MetroCluster"](#) .

È possibile confrontare la configurazione MetroCluster con i requisiti in ["Documentazione MetroCluster"](#) per determinare se la modifica o l'aggiornamento dei componenti nella configurazione MetroCluster potrebbe migliorare le prestazioni del carico di lavoro. Questo confronto può aiutarti a rispondere alle seguenti domande:

- I controller sono adatti ai tuoi carichi di lavoro?
- Hai bisogno di aggiornare i tuoi pacchetti ISL a una larghezza di banda maggiore per gestire una maggiore produttività?
- È possibile modificare i crediti buffer-to-buffer (BBC) sui propri switch per aumentare la larghezza di banda?
- Se i tuoi carichi di lavoro hanno un'elevata velocità di scrittura su unità a stato solido (SSD), devi aggiornare i tuoi bridge FC-SAS per adattarli alla velocità?

Informazioni correlate

- Per informazioni sulla sostituzione o l'aggiornamento dei componenti MetroCluster , vedere ["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 IP MetroCluster mediante switchover e switchback"](#)

Spostare i carichi di lavoro su un aggregato diverso

È possibile utilizzare Unified Manager per identificare un aggregato meno occupato rispetto a quello in cui risiedono attualmente i carichi di lavoro, quindi è possibile spostare i volumi o le LUN selezionati su tale aggregato. Spostando i carichi di lavoro ad alte prestazioni su un aggregato meno utilizzato o su un aggregato con storage flash abilitato, è possibile ottenere prestazioni più efficienti del carico di lavoro.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devi aver registrato il nome dell'aggregato che presenta attualmente un problema di prestazioni.
- 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 sulle prestazioni.

Questi passaggi ti aiutano a identificare le seguenti risorse in modo da poter spostare i carichi di lavoro ad alte prestazioni su un aggregato meno utilizzato:

- Gli aggregati sullo stesso cluster che sono meno utilizzati
- I volumi più performanti sull'aggregato attuale

Passi

1. Identificare l'aggregato nel cluster che è meno utilizzato:

a. Dalla pagina dei dettagli **Evento**, fare clic sul nome del cluster su cui risiede l'aggregato.

I dettagli del cluster vengono visualizzati nella pagina di destinazione Prestazioni/Cluster.

b. Nella pagina **Riepilogo**, fare clic su **Aggregati** nel riquadro **Oggetti gestiti**.

Viene visualizzato l'elenco degli aggregati presenti in questo cluster.

c. Fare clic sulla colonna **Utilizzo** per ordinare gli aggregati in base al loro utilizzo minore.

È anche possibile identificare gli aggregati che hanno la maggiore **Capacità libera**. Viene fornito un elenco di potenziali aggregati su cui potresti voler spostare i carichi di lavoro.

d. Annotare il nome dell'aggregato su cui si desidera spostare i carichi di lavoro.

2. Identificare i volumi ad alte prestazioni dall'aggregato che ha ricevuto l'evento:

a. Fare clic sull'aggregato che presenta il problema di prestazioni.

I dettagli aggregati vengono visualizzati nella pagina Performance/Aggregate Explorer.

b. Dal selettore **Intervallo di tempo**, seleziona **Ultimi 30 giorni**, quindi fai clic su **Applica intervallo**.

Ciò consente di visualizzare un periodo di cronologia delle prestazioni più lungo rispetto alle 72 ore predefinite. Si desidera spostare un volume che utilizza molte risorse in modo continuativo, non solo nelle ultime 72 ore.

c. Dal controllo **Visualizza e confronta**, seleziona **Volumi su questo aggregato**.

Viene visualizzato un elenco dei volumi FlexVol e dei volumi costituenti FlexGroup su questo aggregato.

d. Ordina i volumi in base al valore MB/s più alto e poi in base al valore IOPS più alto per visualizzare i volumi con le prestazioni più elevate.

e. Annotare i nomi dei volumi che si desidera spostare in un aggregato diverso.

3. Sposta i volumi ad alte prestazioni nell'aggregato che hai identificato come a basso utilizzo.

È possibile eseguire l'operazione di spostamento utilizzando ONTAP System Manager, OnCommand

Workflow Automation, i comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, controlla se stai ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostare i carichi di lavoro su 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, e quindi spostare i volumi selezionati su tale aggregato. Spostando i carichi di lavoro ad alte prestazioni su un aggregato su un nodo meno trafficato, i carichi di lavoro su entrambi i nodi possono funzionare in modo più efficiente.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devi aver registrato il nome del nodo che attualmente presenta un problema di prestazioni.
- È necessario aver registrato la data e l'ora in cui il nodo ha ricevuto l'evento di prestazione.
- Unified Manager deve aver raccolto e analizzato i dati sulle prestazioni per un mese o più.

Questa procedura consente di identificare le seguenti risorse in modo da poter spostare carichi di lavoro ad alte prestazioni su un nodo meno utilizzato:

- I nodi sullo stesso cluster che hanno la maggiore capacità di prestazioni libera
- Gli aggregati sul nuovo nodo che hanno la maggiore capacità di prestazioni libere
- I volumi più performanti sul nodo corrente

Passi

1. Identificare un nodo nel cluster che abbia la maggiore capacità di prestazioni libera:

a. Nella pagina **Dettagli evento**, fare clic sul nome del cluster su cui risiede il nodo.

I dettagli del cluster vengono visualizzati nella pagina di destinazione Prestazioni/Cluster.

b. Nella scheda **Riepilogo**, fare clic su **Nodi** nel riquadro **Oggetti gestiti**.

Viene visualizzato l'elenco dei nodi di questo cluster.

c. Fare clic sulla colonna **Capacità di prestazioni utilizzata** per ordinare i nodi in base alla percentuale minima utilizzata.

Viene fornito un elenco di potenziali nodi su cui potresti voler spostare i carichi di lavoro.

d. Annotare il nome del nodo su cui si desidera spostare i carichi di lavoro.

2. Identificare un aggregato sul nuovo nodo che sia il meno utilizzato:

a. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati** e selezionare **Prestazioni > Tutti gli aggregati** dal menu Visualizza.

Viene visualizzata la vista Prestazioni: Tutti gli aggregati.

b. Fare clic su **Filtro**, selezionare **Nodo** dal menu a discesa a sinistra, digitare il nome del nodo nel

campo di testo, quindi fare clic su **Applica filtro**.

Viene nuovamente visualizzata la vista Prestazioni: tutti gli aggregati con l'elenco degli aggregati disponibili su questo nodo.

- c. Fare clic sulla colonna **Capacità di prestazione utilizzata** per ordinare gli aggregati in base a quelli meno utilizzati.

Viene fornito un elenco di potenziali aggregati su cui potresti voler spostare i carichi di lavoro.

- d. Annotare il nome dell'aggregato su cui si desidera spostare i carichi di lavoro.

3. Identificare i carichi di lavoro ad alte prestazioni dal nodo che ha ricevuto l'evento:

- a. Torna alla pagina **Dettagli evento** dell'evento.
- b. Nel campo **Volumi interessati**, fare clic sul collegamento per il numero di volumi.

La vista 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.

Viene fornito un elenco di potenziali volumi che potresti voler spostare.

- d. Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti su cui risiedono.

4. Spostare i volumi negli aggregati identificati come dotati della maggiore capacità di prestazioni libere sul nuovo nodo.

È possibile eseguire l'operazione di spostamento utilizzando ONTAP System Manager, OnCommand Workflow Automation, i comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, puoi verificare se stai ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostare i carichi di lavoro su 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, e quindi spostare i volumi selezionati su tale aggregato. Spostando i carichi di lavoro ad alte prestazioni su un aggregato su un nodo meno trafficato, i carichi di lavoro su entrambi i nodi possono funzionare in modo più efficiente.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Devi aver registrato il nome del nodo che attualmente presenta un problema di prestazioni.
- È necessario aver registrato la data e l'ora in cui il nodo ha ricevuto l'evento di prestazione.
- Unified Manager deve aver raccolto e analizzato almeno un mese di dati sulle prestazioni.

Questi passaggi ti aiutano a identificare le seguenti risorse in modo da poter spostare carichi di lavoro ad alte prestazioni su un nodo meno utilizzato:

- I nodi sullo stesso cluster che sono meno utilizzati

- Gli aggregati sul nuovo nodo che sono meno utilizzati
- I volumi più performanti sul nodo corrente

Passi

1. Identificare un nodo nel cluster che è il meno utilizzato:

- Dalla pagina dei dettagli **Evento**, fare clic sul nome del cluster su cui risiede il nodo.

I dettagli del cluster vengono visualizzati nella pagina di destinazione Prestazioni/Cluster.

- Nella pagina **Riepilogo**, fare clic su **Nodi** nel riquadro **Oggetti gestiti**.

Viene visualizzato l'elenco dei nodi di questo cluster.

- Fare clic sulla colonna **Utilizzo** per ordinare i nodi in base al loro utilizzo minore.

È anche possibile identificare i nodi che hanno la maggiore **Capacità libera**. Viene fornito un elenco di potenziali nodi su cui potresti voler spostare i carichi di lavoro.

- Annotare il nome del nodo su cui si desidera spostare i carichi di lavoro.

2. Identificare un aggregato sul nuovo nodo che sia il meno utilizzato:

- Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati** e selezionare **Prestazioni > Tutti gli aggregati** dal menu Visualizza.

Viene visualizzata la vista Prestazioni: Tutti gli aggregati.

- Fare clic su **Filtro**, selezionare **Nodo** dal menu a discesa a sinistra, digitare il nome del nodo nel campo di testo, quindi fare clic su **Applica filtro**.

Viene nuovamente visualizzata la vista Prestazioni: tutti gli aggregati con l'elenco degli aggregati disponibili su questo nodo.

- Fare clic sulla colonna **Utilizzo** per ordinare gli aggregati in base al loro utilizzo minore.

È anche possibile identificare gli aggregati che hanno la maggiore **Capacità libera**. Viene fornito un elenco di potenziali aggregati su cui potresti voler spostare i carichi di lavoro.

- Annotare il nome dell'aggregato su cui si desidera spostare i carichi di lavoro.

3. Identificare i carichi di lavoro ad alte prestazioni dal nodo che ha ricevuto l'evento:

- Torna alla pagina dei dettagli dell'evento.
- Nel campo **Volumi interessati**, fare clic sul collegamento per il numero di volumi.

La vista Prestazioni: Tutti i volumi viene visualizzata con un elenco filtrato dei volumi su quel nodo.

- Fare clic sulla colonna **Capacità totale** per ordinare i volumi in base allo spazio allocato più grande.

Viene fornito un elenco di potenziali volumi che potresti voler spostare.

- Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti su cui risiedono.

4. Sposta i volumi sugli aggregati identificati come poco utilizzati sul nuovo nodo.

È possibile eseguire l'operazione di spostamento utilizzando ONTAP System Manager, OnCommand Workflow Automation, i comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, controlla se stai ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostare i carichi di lavoro su un nodo in una coppia HA diversa

È possibile utilizzare Unified Manager per identificare un aggregato su un nodo in una coppia ad alta disponibilità (HA) diversa che dispone di una maggiore capacità di prestazioni libera rispetto alla coppia HA in cui sono attualmente in esecuzione i carichi di lavoro. È quindi possibile spostare i volumi selezionati negli aggregati sulla nuova coppia HA.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Il tuo 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 nella coppia HA che presentano attualmente un problema di prestazioni.
- È necessario aver registrato la data e l'ora in cui i nodi hanno ricevuto l'evento di prestazione.
- Unified Manager deve aver raccolto e analizzato i dati sulle prestazioni per un mese o più.

Spostando i carichi di lavoro ad alte prestazioni su un aggregato su un nodo con maggiore capacità di prestazioni libera, i carichi di lavoro su entrambi i nodi funzionano in modo più efficiente. Questa procedura consente di identificare le seguenti risorse in modo da poter spostare carichi di lavoro ad alte prestazioni su un nodo con maggiore capacità di prestazioni libera su una coppia HA diversa:

- I nodi in una coppia HA diversa sullo stesso cluster che hanno la maggiore capacità di prestazioni libera
- Gli aggregati sui nuovi nodi che hanno la maggiore capacità di prestazioni libere
- I volumi più performanti sui nodi attuali

Passi

1. Identificare i nodi che fanno parte di una diversa coppia HA sullo stesso cluster:

- a. Nella pagina **Dettagli evento**, fare clic sul nome del cluster in cui risiedono i nodi.

I dettagli del cluster vengono visualizzati nella pagina di destinazione Prestazioni/Cluster.

- b. Nella pagina **Riepilogo**, fare clic su **Nodi** nel riquadro **Oggetti gestiti**.

L'elenco dei nodi su questo cluster viene visualizzato nella vista Prestazioni: Tutti i nodi.

- c. Annotare i nomi dei nodi che si trovano in coppie HA diverse dalla coppia HA che attualmente presenta un problema di prestazioni.

2. Identificare un nodo nella nuova coppia HA che abbia la maggiore capacità di prestazioni libera:

- a. Nella vista **Prestazioni: tutti i nodi**, fare clic sulla colonna **Capacità di prestazioni utilizzata** per ordinare i nodi in base alla percentuale minima utilizzata.

Viene fornito un elenco di potenziali nodi su cui potresti voler spostare i carichi di lavoro.

- b. Annotare il nome del nodo su una coppia HA diversa su cui si desidera spostare i carichi di lavoro.
3. Identificare un aggregato sul nuovo nodo che abbia la maggiore capacità di prestazioni libera:
 - a. Nella vista **Prestazioni: Tutti i nodi**, fare clic sul nodo.

I dettagli del nodo vengono visualizzati nella pagina Prestazioni/Esplora nodi.

- b. Nel menu **Visualizza e confronta**, seleziona **Aggregati su questo nodo**.

Gli aggregati su questo nodo vengono visualizzati nella griglia.

- c. Fare clic sulla colonna **Capacità di prestazione utilizzata** per ordinare gli aggregati in base a quelli meno utilizzati.

Viene fornito un elenco di potenziali aggregati su cui potresti voler spostare i carichi di lavoro.

- d. Annotare il nome dell'aggregato su cui si desidera spostare i carichi di lavoro.

4. Identificare i carichi di lavoro ad alte prestazioni dai nodi che hanno ricevuto l'evento:

- a. Torna alla pagina dei dettagli dell'evento.
 - b. Nel campo **Volumi interessati**, fare clic sul collegamento per il numero di volumi per il primo nodo.

La vista 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.

Viene fornito un elenco di potenziali volumi che potresti voler spostare.

- d. Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti su cui risiedono.
 - e. Eseguire i passaggi 4c e 4d per il secondo nodo che faceva parte di questo evento per identificare anche i possibili volumi che si desidera spostare da quel nodo.

5. Spostare i volumi negli aggregati identificati come dotati della maggiore capacità di prestazioni libere sul nuovo nodo.

È possibile eseguire l'operazione di spostamento utilizzando ONTAP System Manager, OnCommand Workflow Automation, i comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, puoi verificare se stai ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostare i carichi di lavoro su un altro nodo in una coppia HA diversa

È possibile utilizzare Unified Manager per identificare un aggregato su un nodo in una coppia HA diversa che sia meno occupata della coppia HA in cui sono attualmente in esecuzione i carichi di lavoro. È quindi possibile spostare i volumi selezionati negli aggregati sulla nuova coppia HA. Spostando i carichi di lavoro ad alte prestazioni su un aggregato su un nodo meno trafficato, i carichi di lavoro su entrambi i nodi possono funzionare in modo più efficiente.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

- Il cluster deve essere composto da almeno due coppie HA; non è possibile utilizzare questo processo di ripristino se nel cluster è presente una sola coppia HA.
- È necessario aver registrato i nomi dei due nodi nella coppia HA che attualmente presentano problemi di prestazioni.
- È necessario aver registrato la data e l'ora in cui i nodi hanno ricevuto l'evento di prestazione.
- Unified Manager deve aver raccolto e analizzato almeno un mese di dati sulle prestazioni.

Questi passaggi ti aiutano a identificare le seguenti risorse in modo da poter spostare carichi di lavoro ad alte prestazioni su 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 meno utilizzati
- I volumi più performanti sui nodi attuali

Passi

1. Identificare i nodi che fanno parte di una diversa coppia HA sullo stesso cluster:

- Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster** e selezionare **Prestazioni > Tutti i cluster** dal menu Visualizza.

Viene visualizzata la vista Prestazioni: tutti i cluster.

- Fare clic sul numero nel campo **Conteggio nodi** per il cluster corrente.

Viene visualizzata la vista Prestazioni: Tutti i nodi.

- Annotare i nomi dei nodi che si trovano in coppie HA diverse dalla coppia HA che attualmente presenta il problema di prestazioni.

2. Identificare un nodo nella nuova coppia HA che sia il meno utilizzato:

- Fare clic sulla colonna **Utilizzo** per ordinare i nodi in base al loro utilizzo minore.

È anche possibile identificare i nodi che hanno la maggiore **Capacità libera**. Viene fornito un elenco di potenziali nodi su cui potresti voler spostare i carichi di lavoro.

- Annotare il nome del nodo su cui si desidera spostare i carichi di lavoro.

3. Identificare un aggregato sul nuovo nodo che sia il meno utilizzato:

- Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati** e selezionare **Prestazioni > Tutti gli aggregati** dal menu Visualizza.

Viene visualizzata la vista Prestazioni: Tutti gli aggregati.

- Fare clic su **Filtro**, selezionare **Nodo** dal menu a discesa a sinistra, digitare il nome del nodo nel campo di testo, quindi fare clic su **Applica filtro**.

Viene nuovamente visualizzata la vista Prestazioni: tutti gli aggregati con l'elenco degli aggregati disponibili su questo nodo.

- Fare clic sulla colonna **Utilizzo** per ordinare gli aggregati in base al loro utilizzo minore.

È anche possibile identificare gli aggregati che hanno la maggiore **Capacità libera**. Viene fornito un elenco di potenziali aggregati su cui potresti voler spostare i carichi di lavoro.

- d. Annotare il nome dell'aggregato su cui si desidera spostare i carichi di lavoro.
4. Identificare i carichi di lavoro ad alte prestazioni dai nodi che hanno ricevuto l'evento:
- Torna alla pagina dei dettagli dell'evento.
 - Nel campo **Volumi interessati**, fare clic sul collegamento per il numero di volumi per il primo nodo.

La vista Prestazioni: Tutti i volumi viene visualizzata con un elenco filtrato dei volumi su quel nodo.
 - Fare clic sulla colonna **Capacità totale** per ordinare i volumi in base allo spazio allocato più grande.

Viene fornito un elenco di potenziali volumi che potresti voler spostare.
 - Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti su cui risiedono.
 - Eseguire i passaggi 4c e 4d per il secondo nodo che faceva parte di questo evento per identificare anche i possibili volumi che si desidera spostare da quel nodo.
5. Sposta i volumi sugli aggregati identificati come poco utilizzati sul nuovo nodo.

È possibile eseguire l'operazione di spostamento utilizzando ONTAP System Manager, OnCommand Workflow Automation, i comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, controlla se stai ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Utilizzare le impostazioni dei criteri QoS per dare priorità al lavoro su questo nodo

È possibile impostare un limite su un gruppo di policy QoS per controllare il limite di I/O al secondo (IOPS) o di throughput 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 proprie esigenze, è possibile aumentare il limite impostato o spostare i carichi di lavoro in un gruppo di policy nuovo o esistente che abbia il limite desiderato.

Se un evento di prestazioni su un nodo è causato da carichi di lavoro che utilizzano eccessivamente le risorse del nodo, la descrizione dell'evento nella pagina Dettagli evento visualizza un collegamento all'elenco dei volumi coinvolti. Nella pagina Prestazioni/Volumi, è possibile ordinare i volumi interessati in base a IOPS e MBps per vedere quali carichi di lavoro hanno l'utilizzo più elevato che potrebbe aver contribuito all'evento.

Assegnando i volumi che stanno utilizzando eccessivamente le risorse del nodo a un'impostazione di gruppo di policy più restrittiva, il gruppo di policy limita i carichi di lavoro per limitarne l'attività, il che può ridurre l'utilizzo delle risorse su quel nodo.

È possibile utilizzare ONTAP System Manager o i comandi ONTAP per gestire i gruppi di policy, incluse le seguenti attività:

- Creazione di un gruppo di policy
- Aggiunta o rimozione di carichi di lavoro in un gruppo di policy
- Spostamento di un carico di lavoro tra gruppi di policy
- Modifica del limite di throughput di un gruppo di policy

Rimuovere volumi e LUN inattivi

Se lo spazio libero aggregato viene identificato come un problema, è possibile cercare volumi e LUN inutilizzati ed eliminarli dall'aggregato. Ciò può contribuire ad alleviare il problema dello spazio su disco insufficiente.

Se un evento di prestazioni su un aggregato è causato da spazio su disco insufficiente, esistono alcuni modi per determinare quali volumi e LUN non vengono più utilizzati.

Per identificare i volumi non utilizzati:

- 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 Prestazioni: Tutti i volumi. Da lì è possibile ordinare i volumi interessati in base a **IOPS** per vedere quali volumi non sono stati attivi.

Per identificare i LUN non utilizzati:

1. Nella pagina Dettagli evento, annotare il nome dell'aggregato su cui si è verificato l'evento.
2. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > LUN** e selezionare **Prestazioni > Tutti i LUN** dal menu Visualizza.
3. Fare clic su **Filtro**, selezionare **Aggregato** dal menu a discesa a sinistra, digitare il nome dell'aggregato nel campo di testo, quindi fare clic su **Applica filtro**.
4. Ordinare l'elenco risultante delle LUN interessate in base a **IOPS** per visualizzare le LUN non attive.

Dopo aver identificato i volumi e i LUN non utilizzati, è possibile utilizzare ONTAP System Manager 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 aumentarne la capacità di archiviazione e le prestazioni. Dopo aver aggiunto i dischi, si nota un miglioramento delle prestazioni solo dopo aver ricostruito l'aggregato.

Quando si riceve un evento soglia definito dal sistema nella pagina Dettagli evento, il testo della descrizione dell'evento elenca il nome dell'aggregato che presenta 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 acquistarne altri. È possibile utilizzare ONTAP System Manager o i comandi ONTAP per aggiungere dischi a un aggregato.

["Rapporto tecnico 3838: Guida alla configurazione del sottosistema di archiviazione"](#)

Impostare una connessione tra un server Unified Manager e un provider di dati esterno

Una connessione tra un server Unified Manager e un provider di dati esterno consente di inviare dati sulle prestazioni del cluster a un server esterno, in modo che i gestori

dell'archiviazione possano tracciare le metriche delle prestazioni utilizzando software di terze parti.

Una connessione tra un server Unified Manager e un fornitore di dati esterno viene stabilita tramite l'opzione di menu denominata "Fornitore di dati esterno" nella console di manutenzione.

Dati sulle prestazioni che possono essere inviati a un server esterno

Unified Manager raccoglie una serie di dati sulle prestazioni da tutti i cluster monitorati. È possibile inviare gruppi specifici di dati a un server esterno.

A seconda dei dati sulle prestazioni che si desidera rappresentare graficamente, è possibile scegliere di inviare uno dei seguenti gruppi di statistiche:

Gruppo di statistica	Dati inclusi	Dettagli
Monitoraggio delle prestazioni	Statistiche sulle prestazioni di alto livello per i seguenti oggetti: • LUN • Volumi	Questo gruppo fornisce IOPS o latenza totali per tutti i 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 statistiche di utilizzo per il nodo e aggrega le risorse fisiche in tutti i cluster monitorati. Fornisce inoltre le statistiche raccolte nel gruppo Performance Monitor.
Approfondimento	Statistiche di lettura/scrittura di basso livello e per protocollo per tutti gli oggetti tracciati: • Nodi • Aggregati • LUN • Volumi • Dischi • LIF • Porte/NIC	Questo gruppo fornisce analisi di lettura/scrittura e per protocollo per tutti e sette i tipi di oggetti tracciati 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 di un oggetto cluster viene modificato sul sistema di archiviazione, sia il vecchio che il nuovo oggetto conterranno dati sulle prestazioni sul server esterno (denominato "metric_path"). I due oggetti non sono correlati come se fossero lo 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 per il vecchio volume e i nuovi dati sulle prestazioni per il nuovo volume.

Per l'elenco di tutti i contatori delle prestazioni che possono essere inviati a un fornitore di dati esterno, consultare l'articolo 30096 della Knowledge Base.

"Contatori delle prestazioni di Unified Manager che possono essere esportati in un provider di dati esterno"

Configura Graphite per ricevere dati sulle prestazioni da Unified Manager

Graphite è uno strumento software aperto per la raccolta e la rappresentazione grafica dei dati sulle prestazioni provenienti dai sistemi informatici. Il server e il software Graphite devono essere configurati correttamente per ricevere dati statistici da Unified Manager.

NetApp non testa né verifica versioni specifiche di Graphite o di altri strumenti di terze parti.



Il server Graphite non riceve dati sulle prestazioni per i volumi da Unified Manager.

Dopo aver installato Graphite secondo le istruzioni di installazione, è necessario apportare le seguenti modifiche per supportare il trasferimento dei dati statistici da Unified Manager:

- Nel `/opt/graphite/conf/carbon.conf` file, il numero massimo di file che possono essere creati 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 statistici selezionati per l'invio, potrebbero essere necessari inizialmente migliaia di nuovi file. Con 200 file al minuto, potrebbero volerci 15 minuti o più prima che tutti i file metrici vengano inizialmente creati. Dopo aver creato tutti i file metrici univoci, questo parametro non è più rilevante.

- Se si esegue Graphite su un server distribuito utilizzando un indirizzo IPv6, il valore per `LINE_RECEIVER_INTERFACE` in `/opt/graphite/conf/carbon.conf` il file deve essere modificato da "0.0.0.0" a "::"(`LINE_RECEIVER_INTERFACE = ::`)
- Nel `/opt/graphite/conf/storage-schemas.conf` file, il `retentions` deve essere utilizzato per impostare la frequenza su 5 minuti e il periodo di conservazione sul numero di giorni rilevante per il tuo 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, una sezione è definita per Unified Manager utilizzando `pattern` parametro e i valori impostano la frequenza iniziale a 5 minuti e il periodo di conservazione a 100 giorni: **[OPM]**

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



Se il tag del fornitore predefinito viene modificato da "netapp-performance" a qualcosa di diverso, tale modifica deve essere riflessa nel `pattern` anche il parametro.



Se il server Graphite non è disponibile quando il server Unified Manager tenta di inviare dati sulle prestazioni, i dati non vengono inviati e si verificherà un'interruzione nei dati raccolti.

Configurare una connessione da un server Unified Manager a un provider di dati esterno

Unified Manager può inviare dati sulle prestazioni del cluster a un server esterno. È possibile specificare il tipo di dati statistici da inviare e l'intervallo di invio dei dati.

Prima di iniziare

- 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 fornitore 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 possano ricevere dati statistici dal server Unified Manager.
- Devi sapere quale gruppo di statistiche vuoi inviare:
 - PERFORMANCE_INDICATOR: statistiche del monitoraggio delle prestazioni
 - RESOURCE_UTILIZATION: statistiche di utilizzo delle risorse e monitoraggio delle prestazioni
 - 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 inviata durante ogni 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 a 10 o 15 minuti, è necessario modificare l'intervallo di trasmissione in modo che sia uguale o maggiore dell'intervallo di raccolta di Unified Manager.

È possibile configurare una connessione tra un server Unified Manager e un server provider di dati esterno.

Passi

1. Accedere come utente addetto alla 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 **Fornitore di dati esterno**.

Viene visualizzato il menu Connessione al server esterno.

3. Digitare il numero dell'opzione di menu **Aggiungi/Modifica connessione server**.

Vengono visualizzate le informazioni sulla connessione corrente al server.

4. Quando richiesto, digitare **y** per continuare.

5. Quando richiesto, immettere 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 inserite siano corrette.
7. Premere un tasto qualsiasi per tornare al menu Connessione server esterno.
8. Digitare il numero dell'opzione di menu **Modifica configurazione server**.

Vengono visualizzate le informazioni sulla configurazione corrente del server.

9. Quando richiesto, digitare **y** per continuare.
10. Quando richiesto, immettere il tipo di statistiche da inviare, l'intervallo di tempo in cui inviare le statistiche e se si desidera abilitare la trasmissione delle statistiche ora:

Per..	Entra...
ID gruppo statistiche	0- PERFORMANCE_INDICATOR (predefinito) 1- UTILIZZO_RISORSE 2- DRILL_DOWN
Etichetta del fornitore	Nome descrittivo per la cartella in cui verranno archiviate le statistiche sul server esterno. "netapp-performance" è il nome predefinito, ma è possibile immettere un altro valore. Utilizzando la notazione puntata è possibile definire una struttura gerarchica delle cartelle. Ad esempio, inserendo stats.performance.netapp le statistiche si troveranno in stats > performance > netapp .
Intervallo di trasmissione	5 (predefinito), 10 , O 15 minuti
Abilita/disabilita	0- Disabilita 1- Abilita (predefinito)

11. Quando richiesto, digitare **y** per verificare che le informazioni inserite siano corrette.
12. Premere un tasto qualsiasi per tornare al menu Connessione server esterno.
13. Tipo **x** per uscire dalla console di manutenzione.

Dopo aver configurato la connessione, i dati sulle prestazioni selezionati vengono inviati al server di destinazione nell'intervallo di tempo specificato. Ci vogliono alcuni minuti prima che le metriche inizino ad apparire nello strumento esterno. Potrebbe essere necessario aggiornare il browser per visualizzare le nuove metriche nella gerarchia delle metriche.

Monitorare e gestire lo stato di salute del cluster

Introduzione al monitoraggio dello stato di salute Active IQ Unified Manager

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) consente di monitorare un gran numero di sistemi che eseguono il software ONTAP tramite un'interfaccia utente centralizzata. L'infrastruttura del server Unified Manager offre scalabilità, supporto e funzionalità avanzate di monitoraggio e notifica.

Le funzionalità principali di Unified Manager includono il monitoraggio, l'invio di avvisi, la gestione della disponibilità e della capacità dei cluster, la gestione delle capacità di protezione e il raggruppamento dei dati diagnostici e il loro invio al supporto tecnico.

Puoi utilizzare Unified Manager per monitorare i tuoi cluster. Quando si verificano problemi nel cluster, Unified Manager ti informa sui dettagli di tali problemi tramite eventi. Alcuni eventi forniscono anche un'azione correttiva che puoi intraprendere per risolvere i problemi. È possibile configurare avvisi per gli eventi in modo che, quando si verificano problemi, si venga avvisati tramite e-mail e trap SNMP.

È possibile utilizzare Unified Manager per gestire gli oggetti di archiviazione nel proprio ambiente associandoli ad annotazioni. È possibile creare annotazioni personalizzate e associare dinamicamente cluster, macchine virtuali di archiviazione (SVM) e volumi alle annotazioni tramite regole.

È inoltre possibile pianificare i requisiti di archiviazione degli oggetti del cluster utilizzando le informazioni fornite nei grafici di capacità e integrità per il rispettivo oggetto del cluster.

Capacità fisica e logica

Unified Manager sfrutta i concetti di spazio fisico e logico utilizzati per gli oggetti di archiviazione ONTAP .

- **Capacità fisica:** lo spazio fisico si riferisce ai blocchi fisici di archiviazione utilizzati nel volume. La "capacità fisica utilizzata" è in genere inferiore alla capacità logica utilizzata a causa della riduzione dei dati derivanti dalle funzionalità di efficienza di archiviazione (come deduplicazione 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 può essere utilizzato lo spazio teorico, senza tenere conto dei risultati della deduplicazione o della compressione. Lo "spazio logico utilizzato" è lo spazio fisico utilizzato più i risparmi derivanti dalle funzionalità di efficienza di archiviazione (come deduplicazione e compressione) che sono state configurate. Questa misurazione appare spesso maggiore della capacità fisica utilizzata perché 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 di archiviazione in base a unità binarie di 1024 (2^{10}) byte. In ONTAP 9.10.0 e nelle 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 la velocità effettiva continuano a essere kilobyte al secondo (Kbps), megabyte al secondo (Mbps), gigabyte al secondo (Gbps) o terabyte al 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
tubercolosi	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 byte

Funzionalità di monitoraggio dello stato di Unified Manager

Unified Manager è basato su un'infrastruttura server che offre scalabilità, supporto 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, ripiani di dischi, coppie SFO, porte e Flash Cache
 - Oggetti logici: cluster, macchine virtuali di archiviazione (SVM), aggregati, volumi, LUN, namespace, qtrees, LIF, copie snapshot, percorsi di giunzione, condivisioni NFS, condivisioni SMB, quote utente e gruppo, gruppi di policy QoS e gruppi di iniziatori
 - Protocolli: CIFS, NFS, FC, iSCSI, NVMe e FCoE
 - Efficienza di archiviazione: aggregati SSD, aggregati Flash Pool, aggregati FabricPool , deduplicazione e compressione
 - Protezione: relazioni SnapMirror (sincrone e asincrone) e relazioni SnapVault
- Visualizzazione dello stato di rilevamento e monitoraggio del cluster
- MetroCluster su configurazioni 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 su FC
- Avvisi, eventi e infrastruttura di soglia migliorati
- LDAP, LDAPS, autenticazione SAML e supporto utente locale
- RBAC (per un set predefinito di ruoli)
- AutoSupport e pacchetto di supporto
- Dashboard migliorata per mostrare la capacità, la disponibilità, la protezione e lo stato delle prestazioni dell'ambiente
- Interoperabilità dello spostamento del volume, cronologia dello spostamento del volume e cronologia delle modifiche del percorso di giunzione
- Area Ambito di impatto che visualizza graficamente le risorse interessate da eventi quali Alcuni dischi

guasti, Mirroring aggregato MetroCluster degradato e Dischi di riserva MetroCluster lasciati indietro

- Area Effetto possibile che mostra l'effetto degli eventi MetroCluster
- Area Azioni correttive suggerite che mostra le azioni che possono essere eseguite per risolvere eventi quali Alcuni dischi non funzionanti, Mirroring aggregato MetroCluster degradato e Dischi di riserva MetroCluster lasciati indietro
- Area Risorse che potrebbero essere interessate che visualizza le risorse che potrebbero essere interessate da eventi quali l'evento Volume offline, l'evento Volume con restrizioni e l'evento Spazio volume a rischio con thin provisioning
- Supporto per SVM con volumi FlexVol o FlexGroup
- Supporto per il monitoraggio dei volumi radice del nodo
- Monitoraggio avanzato delle copie Snapshot, incluso il calcolo dello spazio recuperabile e l'eliminazione delle copie Snapshot
- Annotazioni per gli oggetti di archiviazione
- Creazione e gestione di report sulle informazioni relative agli oggetti di archiviazione, quali capacità fisica e logica, utilizzo, risparmio di spazio, prestazioni ed eventi correlati
- Integrazione con OnCommand Workflow Automation per eseguire flussi di lavoro

Storage Automation Store contiene pacchetti di flussi di lavoro di archiviazione automatizzati certificati NetApp, sviluppati per l'uso con OnCommand Workflow Automation (WFA). È possibile scaricare i pacchetti e poi importarli in WFA per eseguirli. I flussi di lavoro automatizzati sono disponibili qui:

["Negozio di automazione dell'archiviazione"](#)

Interfacce di Unified Manager utilizzate per gestire lo stato del sistema di archiviazione

Queste sezioni contengono informazioni sulle due interfacce utente fornite da Active IQ Unified Manager per la risoluzione dei problemi relativi alla capacità di archiviazione dei dati, alla disponibilità e alla protezione. Le due interfacce utente sono l'interfaccia utente Web di Unified Manager e la console di manutenzione.

Se si desidera utilizzare le funzionalità di protezione in Unified Manager, è necessario installare e configurare anche OnCommand Workflow Automation (WFA).

Interfaccia utente web di Unified Manager

L'interfaccia utente Web di Unified Manager consente all'amministratore di monitorare e risolvere i problemi del cluster relativi alla capacità di archiviazione dei dati, alla disponibilità e alla protezione.

In queste sezioni vengono descritti alcuni flussi di lavoro comuni che un amministratore può seguire per risolvere i problemi di capacità di archiviazione, 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 problemi del sistema operativo, problemi di aggiornamento della versione, problemi di accesso degli utenti e problemi di rete correlati 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 utilizzarle per risolvere i problemi relativi al funzionamento del server Unified Manager.

Gestione e monitoraggio dei cluster e dello stato degli oggetti cluster

Unified Manager utilizza query API periodiche e un motore di raccolta dati per raccogliere dati dai cluster. Aggiungendo cluster al database Unified Manager, è possibile monitorare e gestire tali cluster per individuare eventuali rischi di disponibilità e capacità.

Comprendere il monitoraggio dei cluster

È possibile aggiungere cluster al database Unified Manager per monitorarne 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 tal senso, Unified Manager invia una notifica a un destinatario specificato quando un evento attiva un avviso.

Comprendere i volumi radice del nodo

È possibile monitorare il volume radice del nodo utilizzando Unified Manager. La prassi migliore è che il volume radice del nodo abbia una capacità sufficiente per impedire il blocco del nodo.

Quando la capacità utilizzata del volume radice del nodo supera l'80 percento della capacità totale del volume radice del nodo, viene generato l'evento Spazio volume radice del nodo quasi pieno. È possibile configurare un avviso per l'evento per ricevere una notifica. È possibile adottare misure appropriate per impedire che il nodo si interrompa utilizzando ONTAP System Manager o ONTAP CLI.



La funzionalità di monitoraggio dei volumi radice dei nodi non è disponibile se i cluster eseguono ONTAP versione 9.14.1 o successiva.

Comprendere gli eventi e le soglie per gli aggregati radice del nodo

È possibile monitorare l'aggregato radice del nodo utilizzando Unified Manager. La procedura migliore è quella di effettuare un provisioning approfondito del volume radice nell'aggregato radice per impedire l'arresto del nodo.

Per impostazione predefinita, gli eventi di capacità e prestazioni non vengono generati per gli aggregati radice. Inoltre, i valori soglia utilizzati da Unified Manager non sono applicabili agli aggregati radice del nodo. Solo un rappresentante del supporto tecnico può modificare le impostazioni per la generazione di questi eventi. Quando le impostazioni vengono modificate dal rappresentante del supporto tecnico, i valori di soglia della capacità vengono applicati all'aggregato radice del nodo.

È possibile adottare misure appropriate per impedire l'arresto del nodo utilizzando ONTAP System Manager o ONTAP CLI.



La funzionalità di monitoraggio degli aggregati radice dei nodi non è disponibile se i cluster eseguono ONTAP versione 9.14.1 o successiva.

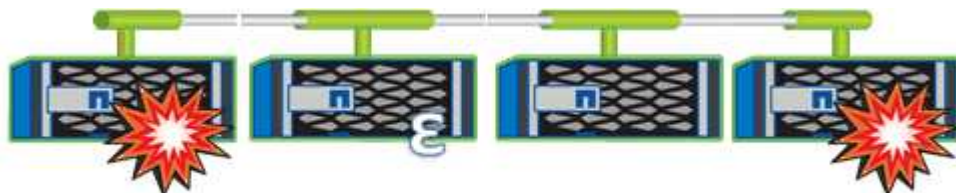
Comprendere il quorum e l'epsilon

Quorum ed epsilon sono misure importanti dello stato di salute e del funzionamento del cluster che, insieme, indicano come i cluster affrontano potenziali sfide in termini di comunicazione e connettività.

Il *quorum* è una precondizione per un cluster pienamente funzionante. Quando un cluster è in quorum, la maggioranza semplice dei nodi è integro e può comunicare tra loro. Quando il quorum viene perso, il cluster perde la capacità di svolgere le normali operazioni del cluster. Solo una raccolta di nodi alla volta può avere il quorum, perché tutti i nodi condividono collettivamente un'unica vista dei dati. Pertanto, se a due nodi non comunicanti è consentito modificare i dati in modi divergenti, non è più possibile riconciliare i dati in un'unica vista dati.

Ogni nodo del cluster partecipa a un protocollo di voto che elegge un nodo master; ogni nodo rimanente è un nodo secondario. Il nodo master è responsabile della sincronizzazione delle informazioni nel cluster. Una volta raggiunto il quorum, questo viene mantenuto tramite votazione continua. Se il nodo master va offline e il cluster è ancora in quorum, un nuovo master viene eletto dai nodi che rimangono online.

Poiché esiste la possibilità di un pareggio in un cluster con un numero pari di nodi, un nodo ha un peso di voto frazionario extra chiamato epsilon. Se la connettività tra due parti uguali di un cluster di grandi dimensioni si interrompe, il gruppo di nodi contenente 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 nodi sono guasti. Tuttavia, poiché uno dei nodi sopravvissuti contiene epsilon, il cluster rimane in quorum anche se non vi è una maggioranza semplice di nodi sani.



Epsilon viene assegnato automaticamente al primo nodo quando viene creato il cluster. Se il nodo che contiene epsilon diventa non funzionante, prende il controllo del suo partner ad alta disponibilità o viene preso in carico dal suo partner ad alta disponibilità, epsilon viene automaticamente riassegnato a un nodo funzionante in una coppia HA diversa.

Mettere offline un nodo può influire sulla capacità del cluster di rimanere in quorum. Pertanto, ONTAP emette un messaggio di avviso se si tenta un'operazione che potrebbe far uscire il cluster dal quorum o portarlo a un'interruzione di corrente dalla 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, presupponendo una connettività affidabile tra i nodi del cluster, un cluster più grande è più stabile di uno più piccolo. Il requisito del quorum, ovvero la maggioranza semplice della metà dei nodi più epsilon, è più facile da mantenere in un cluster di 24 nodi rispetto a un cluster di due nodi.

Un cluster a due nodi presenta alcune sfide particolari per il mantenimento del quorum. I cluster a due nodi utilizzano cluster HA, in cui nessuno dei due nodi detiene epsilon; al contrario, entrambi i nodi vengono interrogati continuamente per garantire che, in caso di guasto di un nodo, l'altro abbia pieno accesso in lettura e scrittura ai dati, nonché accesso alle interfacce logiche e alle funzioni di gestione.

Visualizza l'elenco e i dettagli dei cluster

È possibile utilizzare la vista Integrità: Tutti i cluster per visualizzare l'inventario dei cluster. La vista Capacità: tutti i cluster consente di visualizzare informazioni riepilogative sulla capacità di archiviazione e sull'utilizzo in tutti i cluster.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

È inoltre possibile visualizzare i dettagli dei singoli cluster, ad esempio lo stato di integrità, la capacità, la configurazione, i LIF, i nodi e i dischi del cluster, utilizzando la pagina Dettagli cluster/stato di integrità.

I dettagli nella vista Integrità: Tutti i cluster, nella vista Capacità: Tutti i cluster e nella pagina Dettagli cluster/Integrità ti aiutano a pianificare l'archiviazione. Ad esempio, prima di effettuare il provisioning di un nuovo aggregato, è possibile selezionare un cluster specifico dalla vista Integrità: Tutti i cluster e ottenere i dettagli sulla capacità per determinare se il cluster dispone dello spazio richiesto.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.
2. Nel menu Visualizza, seleziona la vista **Integrità: tutti i cluster** per visualizzare le informazioni sullo stato oppure la vista **Capacità: tutti i cluster** per visualizzare i dettagli sulla capacità di archiviazione e l'utilizzo in tutti i cluster.
3. Fare clic sul nome di un cluster per visualizzare i dettagli completi del cluster nella pagina dei dettagli **Cluster / Integrità**.

Informazioni correlate

- ["Pagina dei dettagli del cluster/salute"](#)
- ["Prestazioni: visualizzazione di tutti i cluster"](#)
- ["Monitoraggio delle configurazioni MetroCluster"](#)
- ["Visualizzazione dello stato di sicurezza per cluster e VM di archiviazione"](#)
- ["Quali criteri di sicurezza vengono valutati"](#)

Controllare lo stato dei cluster in una configurazione MetroCluster

È possibile utilizzare Active IQ Unified Manager (Unified Manager) per verificare lo stato operativo dei cluster e dei relativi componenti nelle configurazioni MetroCluster su FC e MetroCluster su IP. Se i cluster sono stati coinvolti in un evento di prestazioni rilevato da Unified Manager, lo stato di integrità può aiutare a determinare se un problema hardware o software ha contribuito all'evento.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver analizzato un evento di prestazioni per una configurazione MetroCluster e ottenuto il nome del cluster coinvolto.
- Entrambi i cluster nella configurazione MetroCluster su FC e IP devono essere monitorati dalla stessa

istanza di Unified Manager.

Determinare lo stato del cluster in MetroCluster tramite la configurazione FC

Per determinare lo stato di integrità del cluster in una configurazione MetroCluster su FC, seguire questi passaggi.

Passi

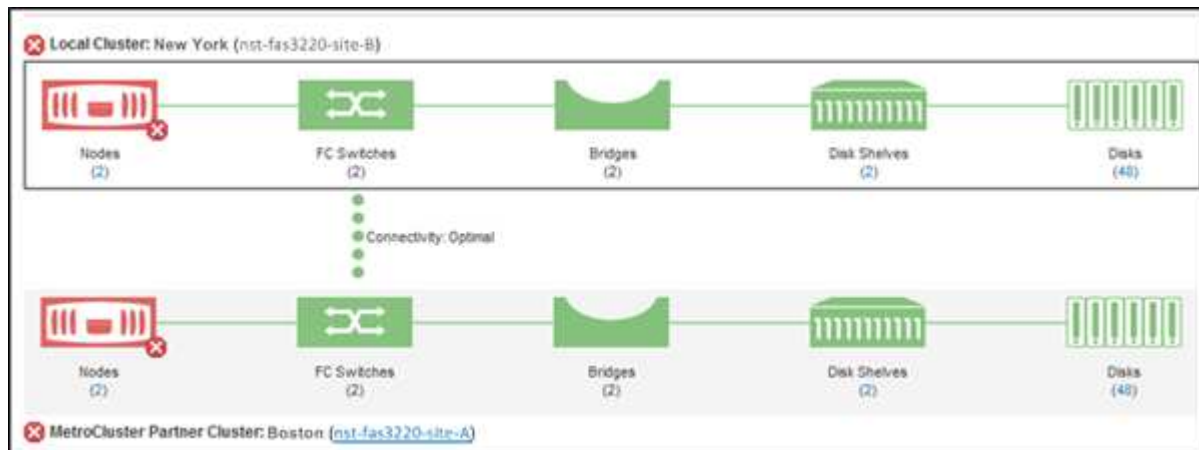
1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi** per visualizzare l'elenco degli eventi.
2. Nel pannello dei filtri, seleziona tutti i filtri MetroCluster nella categoria **Tipo di origine**. Vengono visualizzati tutti gli eventi generati nel tuo ambiente per tutte le configurazioni MetroCluster .
3. Accanto a un evento MetroCluster , fare clic sul nome del cluster.



Se non vengono visualizzati eventi MetroCluster , è possibile utilizzare la barra di ricerca per cercare il nome del cluster coinvolto nell'evento correlato alla configurazione MetroCluster su FC.

Viene visualizzata la vista Integrità: tutti i cluster con informazioni dettagliate sull'evento.

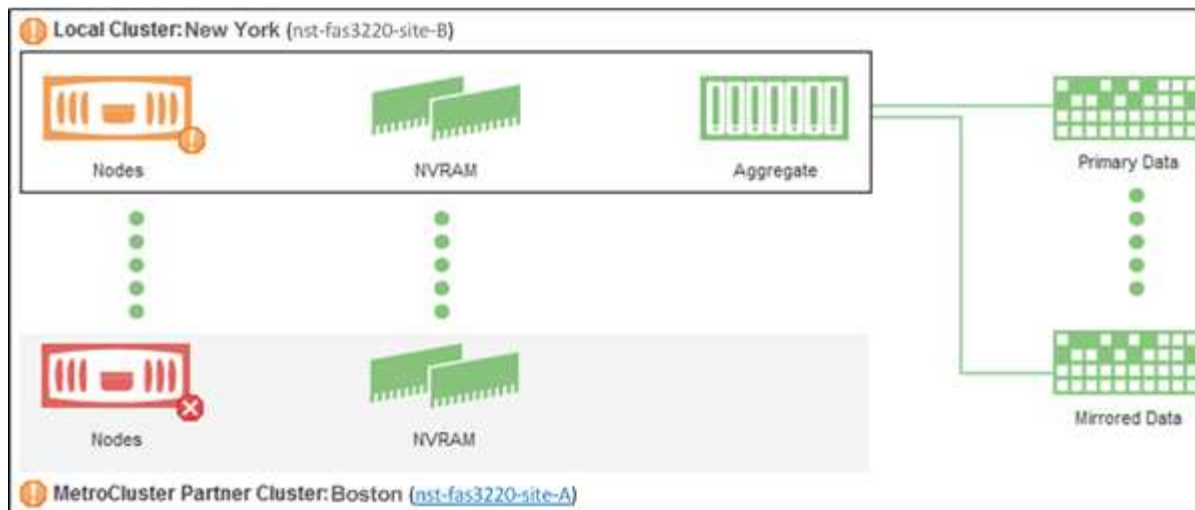
4. Selezionare la scheda ***Connettività MetroCluster *** per visualizzare lo stato della connessione tra il cluster selezionato e il suo cluster partner.



In questo esempio vengono visualizzati i nomi e i componenti del cluster locale e del suo cluster partner. Un'icona gialla o rossa indica un evento di integrità per il componente evidenziato. L'icona Connettività rappresenta il collegamento tra i cluster. È possibile puntare il cursore del mouse su un'icona per visualizzare le informazioni sull'evento oppure fare clic sull'icona per visualizzare gli eventi. Un problema di salute in uno dei due cluster potrebbe aver contribuito all'evento.

Unified Manager monitora il componente NVRAM del collegamento tra i cluster. Se l'icona degli switch FC sul cluster locale o partner oppure l'icona della connettività sono rosse, è possibile che l'evento di prestazioni sia stato causato da un problema di integrità 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 di prestazioni. Se nella pagina non sono presenti icone rosse o gialle, l'evento relativo alle prestazioni potrebbe essere stato causato da un problema di prestazioni nel cluster partner.

Determinare lo stato del cluster nella configurazione MetroCluster su IP

Per determinare lo stato di integrità del cluster in una configurazione MetroCluster su IP, seguire questi passaggi.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi** per visualizzare l'elenco degli eventi.
2. Nel pannello filtro, nella categoria **Tipo di origine**, seleziona **MetroCluster Relationship** filtro. Vengono visualizzati tutti gli eventi generati nel tuo ambiente per tutte le configurazioni MetroCluster .



Se non riesci a visualizzare gli eventi MetroCluster segnalati, puoi utilizzare la barra di ricerca per cercare in base al nome del cluster coinvolto nell'evento correlato alla tua configurazione MetroCluster su IP.

3. Accanto all'evento MetroCluster pertinente, fare clic sul nome del cluster. Viene visualizzata la pagina Cluster con i dettagli di quel cluster. Per informazioni su come determinare i problemi di salute, vedere ["Monitora i problemi di connettività nella configurazione MetroCluster su IP"](#) .

Visualizza lo stato di integrità e capacità di tutti i cluster SAN Array

È possibile utilizzare le pagine Inventario cluster per visualizzare lo stato di integrità e capacità di tutti i cluster SAN Array.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile visualizzare informazioni generali per tutti i cluster SAN Array nella vista Integrità: Tutti i cluster e nella vista Capacità: Tutti i cluster. Inoltre, è possibile visualizzare i dettagli nella pagina Dettagli cluster/stato.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.
2. Assicurarsi che la colonna "Personalità" sia visualizzata nella vista **Salute: Tutti i cluster** oppure aggiungerla utilizzando il controllo **Mostra / Nascondi**.

Questa colonna visualizza "All SAN Array" per i cluster All SAN Array.

3. Rivedi le informazioni.
4. Per visualizzare informazioni sulla capacità di archiviazione in tali cluster, selezionare la vista Capacità: Tutti i cluster.
5. Per visualizzare informazioni dettagliate sullo stato di integrità e sulla capacità di archiviazione in tali cluster, fare clic sul nome di un cluster All SAN Array.

Visualizza i dettagli nelle schede Integrità, Capacità e Nodi nella pagina Dettagli cluster/integrità

Visualizza l'elenco dei nodi e i dettagli

È possibile utilizzare la vista Integrità: Tutti i nodi per visualizzare l'elenco dei nodi nei cluster. È possibile utilizzare la pagina Dettagli cluster/integrità per visualizzare informazioni dettagliate sui nodi che fanno parte del cluster monitorato.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

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 grezza (utilizzabile, di riserva e totale). È inoltre possibile ottenere informazioni sulle coppie HA, sugli scaffali dei dischi e sulle porte.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Nodi**.
2. Nella vista **Stato: Tutti i nodi**, fare clic sul nodo di cui si desidera visualizzare i dettagli.

Le informazioni dettagliate sul nodo selezionato vengono visualizzate nella pagina Dettagli cluster/stato. Nel riquadro di sinistra viene visualizzato l'elenco delle coppie HA. Per impostazione predefinita, la finestra Dettagli HA è aperta e mostra i dettagli sullo stato HA e gli eventi correlati alla coppia HA selezionata.

3. Per visualizzare altri dettagli sul nodo, eseguire l'azione appropriata:

Per visualizzare...	Clic...
Dettagli sugli scaffali dei dischi	Scaffali per dischi.
Informazioni relative al porto	Porte.

Per maggiori informazioni, vedere:

- ["Prestazioni: visualizzazione di tutti i nodi"](#)
- ["Visualizzazione dei valori IOPS disponibili del nodo e dell'aggregato"](#)

- "Visualizzazione dei valori utilizzati per la capacità di prestazione aggregata e del nodo"

Generare un report di inventario hardware per il rinnovo del contratto

È possibile generare un report contenente un elenco completo delle informazioni sui cluster e sui nodi, ad esempio numeri di modello e numeri di serie dell'hardware, tipi e conteggi dei dischi, licenze installate e altro ancora. Questo report è utile per il rinnovo dei contratti all'interno di siti protetti (siti "oscuri") che non sono connessi alla piattaforma NetAppActive IQ.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Nodi**.
2. Vai alla vista **Integrità: Tutti i nodi** o alla vista **Prestazioni: Tutti i nodi**.
3. Selezionare **Report > * > Report inventario hardware***.

Il report dell'inventario hardware viene scaricato come file .csv con informazioni complete aggiornate alla data corrente.

4. Fornisci queste informazioni al tuo referente dell'assistenza NetApp per il rinnovo del contratto.

Visualizza l'elenco e i dettagli delle VM di archiviazione

Dalla vista Integrità: tutte le VM di storage, è possibile monitorare l'inventario delle macchine virtuali di storage (SVM). È possibile utilizzare la pagina Dettagli VM/Stato di archiviazione per visualizzare informazioni dettagliate sulle SVM monitorate.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile visualizzare i dettagli di una SVM, come la capacità, l'efficienza e la configurazione di una SVM. È inoltre possibile visualizzare informazioni sui dispositivi correlati e sugli avvisi correlati per tale SVM.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Per visualizzare i dettagli SVM, scegliere uno dei seguenti metodi:
 - Per visualizzare informazioni sullo stato di integrità di tutte le SVM in tutti i cluster, nel menu Visualizza, selezionare Integrità: vista Tutte le VM di archiviazione.
 - Per visualizzare i dettagli completi, fare clic sul nome della VM di archiviazione.

È anche possibile visualizzare i dettagli completi cliccando su **Visualizza dettagli** nella finestra di dialogo dei dettagli minimi.

3. Visualizza gli oggetti correlati all'SVM facendo clic su **Visualizza correlati** nella finestra di dialogo dei dettagli minimi.

Informazioni correlate

- ["Pagina dei dettagli sullo stato della VM di archiviazione"](#)
- ["Prestazioni: visualizzazione di tutte le VM di archiviazione"](#)
- ["Sicurezza: visualizzazione anti-ransomware"](#)
- ["Visualizzazione dello stato di sicurezza per cluster e VM di archiviazione"](#)
- ["Relazione: visualizzazione di tutte le relazioni"](#)

Visualizza l'elenco aggregato e i dettagli

Dalla vista Salute: Tutti gli aggregati, puoi monitorare il tuo inventario di aggregati. La vista Capacità: tutti gli aggregati consente di visualizzare informazioni sulla capacità e sull'utilizzo degli aggregati in tutti i cluster.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile visualizzare dettagli quali capacità e configurazione aggregate e informazioni sul disco nella pagina Dettagli aggregati/integrità. Se necessario, è possibile utilizzare questi dettagli prima di configurare le impostazioni della soglia.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Per visualizzare i dettagli aggregati, scegli uno dei seguenti metodi:
 - Per visualizzare informazioni sullo stato di integrità di tutti gli aggregati in tutti i cluster, nel menu Visualizza, selezionare Integrità: vista Tutti gli aggregati.
 - Per visualizzare informazioni sulla capacità e l'utilizzo di tutti gli aggregati in tutti i cluster, nel menu Visualizza, selezionare Capacità: vista Tutti gli aggregati.
 - Per visualizzare i dettagli completi, fare clic sul nome dell'aggregato.

È anche possibile visualizzare i dettagli completi cliccando su **Visualizza dettagli** nella finestra di dialogo dei dettagli minimi.

3. Visualizza gli oggetti correlati all'aggregato facendo clic su **Visualizza correlati** nella finestra di dialogo dei dettagli minimi.

Informazioni correlate

- ["Pagina dei dettagli aggregati/sanitari"](#)
- ["Prestazioni: visualizzazione di tutti gli aggregati"](#)
- ["Personalizzazione dei report sulla capacità aggregata"](#)

Visualizza le informazioni sulla capacità FabricPool

È possibile visualizzare le informazioni sulla capacità FabricPool per cluster, aggregati e volumi nelle pagine di inventario e dettagli Capacità e Prestazioni per questi oggetti. Queste pagine visualizzano anche le informazioni sul mirror FabricPool quando è stato

configurato un livello mirror.

Queste pagine visualizzano informazioni quali la capacità disponibile sul livello di prestazioni locale e sul livello cloud, la quantità di capacità utilizzata in entrambi i livelli, quali aggregati sono collegati a un livello cloud e quali volumi implementano le funzionalità FabricPool spostando determinate informazioni sul livello cloud.

Quando un livello cloud viene replicato su un altro provider cloud (il "livello mirror"), entrambi i livelli cloud vengono visualizzati nella pagina dei dettagli Aggregati/Stato.

Passi

1. Eseguire una delle seguenti operazioni:

Per visualizzare le informazioni sulla capacità per...	Fai questo...
Cluster	a. Nella vista Capacità: Tutti i cluster, fare clic su un cluster. b. Nella pagina dei dettagli Cluster/Stato, fare clic sulla scheda Configurazione. Il display mostra i nomi di tutti i livelli cloud a cui è connesso questo 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 dei dettagli Aggregati/Salute, fare clic sulla scheda Capacità. Il display mostra la capacità totale utilizzata nel livello cloud. c. Fare clic sulla scheda 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...	Fai questo...
Volumi	a. Nella vista Capacità: Tutti i volumi, fare clic su un volume in cui appare un nome di policy nel campo "Tiering Policy". b. Nella pagina Dettagli volume/integrità, fare clic sulla scheda Configurazione. Nella schermata viene visualizzato il nome del criterio di suddivisione in livelli 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 dei dischi e degli aggregati"](#) .

Visualizza i dettagli del pool di archiviazione

È possibile visualizzare i dettagli del pool di archiviazione per monitorarne lo stato di integrità, la cache totale e disponibile e le allocazioni utilizzate e disponibili.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Fare clic su un nome aggregato.

Vengono visualizzati i dettagli dell'aggregato selezionato.

3. Fare clic sulla scheda **Informazioni disco**.

Vengono visualizzate informazioni dettagliate sul disco.



La tabella Cache viene visualizzata solo quando l'aggregato selezionato utilizza un pool di archiviazione.

4. Nella tabella Cache, spostare il puntatore sul nome del pool di archiviazione richiesto.

Vengono visualizzati i dettagli del pool di archiviazione.

Visualizza l'elenco dei volumi e i dettagli

Dalla vista Salute: Tutti i volumi, è possibile monitorare l'inventario dei volumi. La vista Capacità: tutti i volumi consente di visualizzare informazioni sulla capacità e sull'utilizzo dei volumi in un cluster.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

È anche possibile utilizzare la pagina Dettagli volume/integrità per visualizzare informazioni dettagliate sui volumi monitorati, tra cui capacità, efficienza, configurazione e protezione dei volumi. È inoltre possibile visualizzare informazioni sui dispositivi correlati e sugli avvisi correlati per un volume specifico.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Per visualizzare i dettagli del volume, scegli uno dei seguenti metodi:
 - Per visualizzare informazioni dettagliate sullo stato di integrità dei volumi in un cluster, nel menu Visualizza selezionare Integrità: vista Tutti i volumi.
 - Per visualizzare informazioni dettagliate sulla capacità e l'utilizzo dei volumi in un cluster, nel menu Visualizza selezionare Capacità: vista Tutti i volumi.
 - Per visualizzare i dettagli completi, fare clic sul nome del volume.

È anche possibile visualizzare i dettagli completi cliccando su **Visualizza dettagli** nella finestra di dialogo dei dettagli minimi.

3. **Facoltativo:** visualizzare gli oggetti correlati al volume facendo clic su **Visualizza correlati** nella finestra di dialogo dei dettagli minimi.

Informazioni correlate

- ["Volume: Pagina dei dettagli sulla salute"](#)
- ["Prestazioni: visualizzazione di tutti i volumi"](#)
- ["Sicurezza: visualizzazione anti-ransomware"](#)
- ["Visualizzazione delle relazioni di protezione del volume"](#)
- ["Creazione di un report per visualizzare i grafici della capacità del volume disponibile"](#)

Visualizza i dettagli sulle azioni NFS

È possibile visualizzare i dettagli su tutte le condivisioni NFS, ad esempio lo 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 Integrità: Tutte le condivisioni NFS per visualizzare tutte le condivisioni NFS su tutti i cluster monitorati e utilizzare la pagina Dettagli VM di archiviazione/Integrità per visualizzare tutte le condivisioni NFS su una specifica macchina virtuale di archiviazione (SVM).

Prima di iniziare

- La licenza NFS deve essere abilitata sul cluster.
- È necessario configurare le interfacce di rete che servono le condivisioni NFS.
- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Fare un passo

1. Nel riquadro di navigazione a sinistra, seguire i passaggi sottostanti a seconda che si desideri visualizzare tutte le condivisioni NFS o solo quelle per una particolare SVM.

A...	Segui questi passaggi...
Visualizza tutte le condivisioni NFS	Fare clic su Archiviazione > Condivisioni NFS
Visualizza le condivisioni NFS per singolo SVM	a. Fare clic su Archiviazione > VM di archiviazione b. Fare clic sull'SVM di cui si desidera visualizzare i dettagli delle condivisioni NFS. c. Nella pagina dei dettagli Storage VM/Health, fare clic sulla scheda Condivisioni NFS.

Per maggiori informazioni, vedere ["Provisioning dei volumi di condivisione file"](#) E ["Provisioning di condivisioni file CIFS e NFS tramite API"](#).

Visualizza i dettagli sulle azioni SMB/CIFS

È possibile visualizzare i dettagli su 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 Integrità: Tutte le condivisioni SMB per visualizzare tutte le condivisioni SMB su tutti i cluster monitorati e utilizzare la pagina Dettagli VM di archiviazione/Integrità per visualizzare tutte le condivisioni SMB su una specifica macchina virtuale di archiviazione (SVM).

Prima di iniziare

- La licenza CIFS deve essere abilitata 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 dell'archiviazione.



Le condivisioni nelle cartelle non vengono visualizzate.

Fare un passo

1. Nel riquadro di navigazione a sinistra, seguire i passaggi sottostanti a seconda che si desideri visualizzare tutte le condivisioni SMB/CIFS o solo le condivisioni per una particolare SVM.

A...	Segui questi passaggi...
Visualizza tutte le azioni SMB/CIFS	Fare clic su Archiviazione > Condivisioni SMB

A...	Segui questi passaggi...
Visualizza le condivisioni SMB/CIFS per singolo SVM	a. Fare clic su Archiviazione > VM di archiviazione b. Fare clic sull'SVM per il quale si desidera visualizzare i dettagli della condivisione SMB/CIFS. c. Nella pagina dei dettagli Storage VM/Health, fare clic sulla scheda Condivisioni SMB.

Per maggiori informazioni, vedere ["Provisioning di condivisioni file CIFS e NFS tramite API"](#).

Visualizza l'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 può essere recuperata se una o più copie Snapshot vengono eliminate e, se necessario, è possibile eliminare le copie Snapshot.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Il volume contenente le copie Snapshot deve essere online.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nella vista **Integrità: Tutti i volumi**, seleziona il volume che contiene le copie Snapshot che desideri visualizzare.
3. Nella pagina dei dettagli **Volume/Salute**, fare clic sulla scheda **Capacità**.
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 Salute/Volumi"](#)

Elimina le copie Snapshot

È possibile eliminare una copia Snapshot per risparmiare spazio o liberare spazio sul disco, oppure è possibile eliminare la copia Snapshot se non è più necessaria.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Il volume deve essere online.

Per eliminare una copia Snapshot occupata o bloccata, è necessario aver rilasciato 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 sta utilizzando tale copia Snapshot.

La copia Snapshot di base è la copia Snapshot utilizzata per creare il volume FlexClone e visualizza 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nella vista **Integrità: Tutti i volumi**, seleziona il volume che contiene le copie Snapshot che desideri visualizzare.

Viene visualizzato l'elenco delle copie Snapshot.

3. Nella pagina dei dettagli **Volume/Salute**, fare clic sulla scheda **Capacità**.
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 **Copie snapshot**, seleziona le copie snapshot che desideri eliminare, quindi fai clic su **Elimina selezionati**.

Calcola lo spazio recuperabile per le copie Snapshot

È possibile calcolare la quantità di spazio su disco che può essere recuperata se vengono eliminate una o più copie Snapshot.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Il volume deve essere online.
- Il volume deve essere un FlexVol volume; questa funzionalità non è supportata con i volumi FlexGroup .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nella vista **Integrità: Tutti i volumi**, seleziona il volume che contiene le copie Snapshot che desideri visualizzare.

Viene visualizzato l'elenco delle copie Snapshot.

3. Nella pagina dei dettagli **Volume/Salute**, fare clic sulla scheda **Capacità**.
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 **Copie snapshot**, seleziona le copie snapshot per le quali desideri calcolare lo spazio recuperabile.

6. Fare clic su **Calcola**.

Viene visualizzato lo spazio recuperabile (in percentuale, KB, MB, GB e così via) sul volume.

7. Per ricalcolare lo spazio recuperabile, selezionare le copie Snapshot desiderate e fare clic su **Ricalcola**.

Descrizione delle finestre e delle finestre di dialogo degli oggetti cluster

È possibile visualizzare tutti i cluster e gli oggetti cluster dalla rispettiva pagina degli oggetti di archiviazione. È anche possibile visualizzare i dettagli dalla pagina dei dettagli dell'oggetto di archiviazione corrispondente. Ora è possibile avviare l'interfaccia utente di System Manager dalle seguenti sezioni ARCHIVIAZIONE e PROTEZIONE dell'INVENTARIO.

- Pagine Inventario cluster, Stato cluster e Prestazioni cluster
- Pagine Inventario aggregato, Salute aggregata e Prestazioni aggregate
- Pagine Inventario del volume, Stato del volume e Prestazioni del volume
- Pagine Inventario nodi e Prestazioni nodi
- Pagine Inventario StorageVM, Integrità StorageVM e Prestazioni StorageVM
- Pagine di relazione di protezione

Flussi di lavoro e attività sanitarie comuni di Unified Manager

Alcuni flussi di lavoro e attività amministrative comuni associati a Unified Manager includono la selezione dei cluster di archiviazione da monitorare; la diagnosi delle condizioni che influiscono negativamente sulla disponibilità, sulla capacità e sulla protezione dei dati; il ripristino dei dati persi; la configurazione e la gestione dei volumi; e il raggruppamento e l'invio dei dati diagnostici al supporto tecnico (quando necessario).

Unified Manager consente agli amministratori di 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 per la risoluzione eventuali problemi specifici che potrebbero presentarsi.

I problemi più importanti relativi a un cluster, a una macchina virtuale di archiviazione (SVM), a un volume o a un volume FlexGroup che influiscono sulla capacità di archiviazione o sulla disponibilità dei dati degli oggetti di archiviazione gestiti vengono visualizzati nei grafici e negli eventi sullo stato del sistema nella pagina Dashboard. Quando vengono identificati problemi critici, questa pagina fornisce collegamenti per supportare flussi di lavoro di risoluzione dei problemi appropriati.

Unified Manager può anche essere incluso nei flussi di lavoro che includono strumenti di gestibilità correlati, come OnCommand Workflow Automation (WFA), per supportare la configurazione diretta delle risorse di archiviazione.

In questo documento vengono descritti i flussi di lavoro comuni relativi alle seguenti attività amministrative:

- Diagnosi e gestione dei problemi di disponibilità

Se un guasto hardware o problemi di configurazione delle risorse di archiviazione causano la visualizzazione di eventi di disponibilità dei dati nella pagina Dashboard, gli amministratori di archiviazione possono seguire i collegamenti incorporati per visualizzare le informazioni di connettività relative alla risorsa di archiviazione interessata, visualizzare suggerimenti per la risoluzione dei problemi e assegnare la risoluzione dei problemi ad altri amministratori.

- Configurazione e monitoraggio degli incidenti di prestazioni

L'amministratore può monitorare e gestire le prestazioni delle risorse del sistema di archiviazione monitorate. Vedi il "[Introduzione al monitoraggio delle prestazioni Active IQ Unified Manager](#)" per maggiori informazioni.

- Diagnosi e gestione dei problemi di capacità del volume

Se nella pagina Dashboard vengono visualizzati problemi di capacità di archiviazione del volume, gli amministratori di archiviazione possono seguire i collegamenti incorporati per visualizzare le tendenze attuali e storiche relative alla capacità di archiviazione del volume interessato, visualizzare suggerimenti per la risoluzione dei problemi e assegnare la risoluzione dei problemi ad altri amministratori.

- Configurazione, monitoraggio e diagnosi dei problemi relativi alla relazione di protezione

Dopo aver creato e configurato le relazioni di protezione, gli amministratori di storage possono visualizzare i potenziali problemi correlati alle relazioni di protezione, lo stato attuale delle relazioni di protezione, le informazioni attuali e storiche sull'esito positivo dei processi di protezione sulle relazioni interessate e suggerimenti per la risoluzione dei problemi. Vedi il "[Creazione, monitoraggio e risoluzione dei problemi delle relazioni di protezione](#)" per maggiori informazioni.

- Creazione di file di backup e ripristino dei dati dai file di backup.

- Associazione di oggetti di archiviazione con annotazioni

Associando gli oggetti di archiviazione alle annotazioni, gli amministratori di archiviazione possono filtrare e visualizzare gli eventi correlati agli oggetti di archiviazione, consentendo loro di stabilire le priorità e risolvere i problemi associati agli eventi.

- Utilizzo delle API REST per gestire i cluster visualizzando le informazioni su integrità, capacità e prestazioni acquisite da Unified Manager. Vedere "[Introduzione alle API REST Active IQ Unified Manager](#)" per maggiori informazioni.

- Invio di un pacchetto di supporto al supporto tecnico

Gli amministratori di storage possono recuperare e inviare un pacchetto di supporto al supporto tecnico tramite 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 di quelle fornite da un messaggio AutoSupport .

Monitorare e risolvere i problemi di disponibilità dei dati

Unified Manager monitora l'affidabilità con cui gli utenti autorizzati possono accedere ai dati archiviati, ti avvisa delle condizioni che bloccano o impediscono tale accesso e ti consente di diagnosticare tali condizioni e di assegnarne e monitorarne la risoluzione.

Gli argomenti del flusso di lavoro sulla disponibilità in questa sezione descrivono esempi di come un amministratore di storage può utilizzare l'interfaccia utente Web di Unified Manager per individuare, diagnosticare e assegnare per la risoluzione condizioni hardware e software che influiscono negativamente sulla disponibilità dei dati.

Esegui la scansione e risolvi le condizioni di inattività del collegamento di interconnessione del failover di archiviazione

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 di archiviazione inattivo. In questo scenario, sei un amministratore che utilizza Unified Manager per analizzare i rischi di failover dell'archiviazione prima di avviare un aggiornamento della versione ONTAP sui tuoi nodi.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Se le interconnessioni di failover dello storage tra i nodi di coppie HA falliscono durante un tentativo di aggiornamento non disruptivo, l'aggiornamento fallisce. Pertanto, è prassi comune che l'amministratore monitori e confermi l'affidabilità del failover di archiviazione sui nodi del cluster destinati all'aggiornamento prima dell'inizio dell'aggiornamento.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.
2. Nella pagina dell'inventario **Gestione eventi**, seleziona **Eventi di disponibilità attiva**.
3. Nella parte superiore della colonna **Nome** della pagina dell'inventario **Gestione eventi**, fare clic su  ed entra `*failover` nella casella di testo per limitare l'evento da visualizzare agli eventi correlati al failover dell'archiviazione.

Vengono visualizzati tutti gli eventi passati relativi alle condizioni di failover dell'archiviazione.

In questo scenario, Unified Manager visualizza l'evento "Storage Failover Interconnect One or More Links Down" nella sezione Incidenti di disponibilità.

4. Se nella pagina dell'inventario **Gestione eventi** vengono visualizzati uno o più eventi correlati al failover dell'archiviazione, procedere come segue:
 - a. Fare clic sul collegamento del titolo dell'evento per visualizzare i dettagli dell'evento stesso.

In questo esempio, fai clic sul titolo dell'evento "Storage Failover Interconnect One or More Links Down".

Viene visualizzata la pagina dei dettagli dell'evento.

- a. Nella pagina Dettagli evento puoi eseguire una o più delle seguenti attività:
 - Esaminare il messaggio di errore nel campo Causa e valutare il problema.
 - Assegna l'evento a un amministratore.
 - Riconosci l'evento.

Informazioni correlate

["Pagina dei dettagli dell'evento"](#)

["Ruoli e capacità degli utenti di Unified Manager"](#)

Eseguire un'azione correttiva per i collegamenti di interconnessione del failover di archiviazione inattivi

Quando si visualizza la pagina Dettagli evento di un evento correlato al failover dell'archiviazione, è possibile esaminare le informazioni di riepilogo della pagina per determinare l'urgenza dell'evento, la possibile causa del problema e la possibile soluzione al problema.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

In questo scenario di esempio, il riepilogo dell'evento fornito nella pagina Dettagli evento contiene le seguenti informazioni sulla condizione di inattività del collegamento di interconnessione del failover di archiviazione:

```
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 di archiviazione, Link1, tra i nodi della coppia HA aardvark e bonobo è inattivo, ma che Link0 tra Apple e Boy è attivo. Poiché un collegamento è attivo, l'accesso alla memoria dinamica remota (RDMA) è ancora funzionante e un processo di failover dell'archiviazione può ancora avere esito positivo.

Tuttavia, per evitare che entrambi i collegamenti falliscano e che la protezione failover dello storage venga completamente disattivata, si decide di diagnosticare ulteriormente il motivo per cui Link1 non funziona.

Passi

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 del failover di archiviazione.

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 Dettagli cluster/stato e vengono visualizzati altri eventi che si sono verificati di recente sulla coppia HA interessata.

2. Per maggiori informazioni relative all'evento, consultare i **Dettagli HA**.

In questo esempio, le informazioni rilevanti si trovano nella tabella Eventi. La tabella mostra l'evento "Storage Failover Connection One or More Link Down", 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 nei dettagli HA, richiedere o completare personalmente un'ispezione fisica e la riparazione del problema di failover dell'archiviazione sui nodi della coppia HA interessati.

Informazioni correlate

["Pagina dei dettagli dell'evento"](#)

["Ruoli e capacità degli utenti di Unified Manager"](#)

Risolvi i problemi di volume offline

Questo flusso di lavoro fornisce un esempio di come valutare e risolvere un evento offline di volume che Unified Manager potrebbe visualizzare nella pagina dell'inventario di Gestione eventi. In questo scenario, sei un amministratore che utilizza Unified Manager per risolvere i problemi di uno o più eventi offline del volume.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

I volumi potrebbero essere segnalati come offline per diversi motivi:

- L'amministratore SVM ha deliberatamente messo offline il volume.
- Il nodo del cluster di hosting del volume è inattivo e anche il failover dello storage sul suo partner di coppia HA non è riuscito.
- La macchina virtuale di archiviazione (SVM) che ospita il volume è arrestata perché il nodo che ospita il volume radice di tale SVM è inattivo.
- L'aggregato di hosting del volume è inattivo a causa del guasto simultaneo di due dischi RAID.

È possibile utilizzare la pagina dell'inventario Gestione eventi e le pagine dei dettagli Cluster/Integrità, Storage VM/Integrità e Volume/Integrità per confermare o eliminare una o più di queste possibilità.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.
2. Nella pagina dell'inventario **Gestione eventi**, seleziona **Eventi di disponibilità attiva**.
3. Fare clic sul collegamento ipertestuale visualizzato per l'evento Volume Offline.

Viene visualizzata la pagina dei dettagli dell'evento per l'incidente di disponibilità.

4. In quella pagina, controlla le note per eventuali indicazioni che l'amministratore SVM abbia portato offline il

volume in questione.

5. Nella pagina dei dettagli dell'**Evento**, puoi rivedere le informazioni per una o più delle seguenti attività:

- Per una possibile guida diagnostica, rivedere le informazioni visualizzate nel campo Causa.

In questo esempio, le informazioni nel campo Causa informano solo che il volume è offline.

- Controllare l'area Note e aggiornamenti per eventuali indicazioni che l'amministratore SVM abbia deliberatamente disattivato il volume in questione.
- Fare clic sull'origine dell'evento, in questo caso il volume segnalato come offline, per ottenere maggiori informazioni su tale volume.
- Assegna l'evento a un amministratore.
- Riconosci l'evento o, se opportuno, contrassegnalo come risolto.

Eseguire azioni diagnostiche per le condizioni di volume offline

Dopo aver navigato alla pagina dei dettagli Volume/Stato di un volume segnalato come offline, è possibile cercare ulteriori informazioni utili per diagnosticare la condizione di offline del volume.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Se il volume segnalato come offline non è stato disattivato deliberatamente, tale volume potrebbe essere offline per diversi motivi.

Partendo dalla pagina dei dettagli Volume/Stato del volume offline, è possibile passare ad altre pagine e riquadri per confermare o eliminare possibili cause:

- Fare clic sui collegamenti della pagina dei dettagli **Volume/Stato** per determinare se il volume è offline perché il suo nodo host è inattivo e anche il failover dello storage sul suo partner di coppia HA non è riuscito.

Vedere ["Determinare se una condizione di volume offline è causata da un nodo inattivo"](#) .

- Fare clic sui collegamenti della pagina dei dettagli **Volume/Integrità** per determinare se il volume è offline e la sua macchina virtuale di archiviazione host (SVM) è arrestata perché il nodo che ospita il volume radice di tale SVM è inattivo.

Vedere ["Determinare se un volume è offline e SVM è arrestato perché un nodo è inattivo"](#) .

- Fare clic sui collegamenti della pagina dei dettagli **Volume/Integrità** per determinare se il volume è offline a causa di dischi danneggiati nel suo aggregato host.

Vedere ["Determinare se un volume è offline a causa di dischi danneggiati in un aggregato"](#) .

Informazioni correlate

["Ruoli e capacità degli utenti di Unified Manager"](#)

Determina se un volume è offline perché il suo nodo host è inattivo

È possibile utilizzare l'interfaccia utente Web di Unified Manager per confermare o escludere la possibilità che un volume sia offline perché il suo nodo host è inattivo e che il failover dello storage sul suo partner di coppia HA non sia riuscito.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per determinare se la condizione di volume offline è causata da un errore del nodo di hosting e dal successivo failover di archiviazione non riuscito, eseguire le seguenti azioni:

Passi

1. Individuare e fare clic sul collegamento ipertestuale visualizzato sotto SVM nel riquadro **Dispositivi correlati** della pagina dei dettagli **Volume / Integrità** del volume offline.

La pagina Dettagli VM di archiviazione/Stato visualizza informazioni sulla macchina virtuale di archiviazione (SVM) che ospita il volume offline.

2. Nel riquadro **Dispositivi correlati** della pagina dei dettagli **VM di archiviazione/integrità**, individuare e fare clic sul collegamento ipertestuale visualizzato in Volumi.

La vista Integrità: Tutti i volumi mostra una tabella di informazioni su tutti i volumi ospitati dall'SVM.

3. Nell'intestazione della colonna Stato della vista **Salute: Tutti i volumi**, fare clic sul simbolo del filtro  , quindi seleziona l'opzione **Offline**.

Vengono elencati solo i volumi SVM che sono offline.

4. Nella vista Salute: Tutti i volumi, fare clic sul simbolo della griglia  e quindi selezionare l'opzione **Nodi cluster**.

Potrebbe essere necessario scorrere la casella di selezione della griglia per individuare l'opzione **Nodi cluster**.

La colonna Nodi cluster viene aggiunta all'inventario dei volumi e visualizza il nome del nodo che ospita ciascun volume offline.

5. Nella vista **Integrità: Tutti i volumi**, individuare l'elenco del volume offline e, nella colonna Nodo cluster, fare clic sul nome del nodo di hosting.

La scheda Nodi nella pagina Dettagli Cluster/Stato 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 vengono indicati nel display.

Dopo aver confermato che la condizione di volume offline esiste perché il suo nodo host è inattivo e il failover dell'archiviazione sul partner della coppia HA non è riuscito, contattare l'amministratore o l'operatore appropriato per riavviare manualmente il nodo inattivo e risolvere il problema di failover dell'archiviazione.

Determina se un volume è offline e il suo SVM è arrestato perché un nodo è inattivo

È possibile utilizzare l'interfaccia utente Web di Unified Manager per confermare o

escludere la possibilità che un volume sia offline perché la sua macchina virtuale di archiviazione host (SVM) è arrestata perché il nodo che ospita il volume radice di tale SVM è inattivo.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per determinare se la condizione di volume offline è causata dall'arresto dell'SVM host perché il nodo che ospita il volume radice di tale SVM è inattivo, eseguire le seguenti azioni:

Passi

1. Individuare e fare clic sul collegamento ipertestuale visualizzato sotto l'SVM nel riquadro **Dispositivi correlati** della pagina dei dettagli **Volume / Integrità** del volume offline.

La pagina dei dettagli Storage VM/Health visualizza lo stato "running" o "stopped" della SVM di hosting. Se lo stato SVM è in esecuzione, la condizione di volume offline non è causata dal fatto che il nodo che ospita il volume radice di tale SVM è inattivo.

2. Se lo stato SVM è arrestato, fare clic su **Visualizza SVM** per identificare ulteriormente la causa dell'arresto dell'SVM di hosting.
3. Nell'intestazione della colonna SVM della vista **Integrità: tutte le VM di archiviazione**, fare clic sul simbolo del filtro  e quindi digitare il nome dell'SVM arrestato.

Le informazioni per tale SVM sono mostrate in una tabella.

4. Nella vista **Stato: tutte le VM di archiviazione**, fare clic su  e quindi selezionare l'opzione **Volume radice**.

La colonna Volume radice viene aggiunta all'inventario SVM e visualizza il nome del volume radice dell'SVM arrestato.

5. Nella colonna Volume radice, fare clic sul nome del volume radice per visualizzare la pagina dei dettagli **VM di archiviazione/integrità** per quel volume.

Se lo stato del volume radice SVM è (Online), la condizione offline del volume originale non è causata dal fatto che il nodo che ospita il volume radice di tale SVM è inattivo.

6. Se lo stato del volume radice SVM è (Offline), individuare e fare clic sul collegamento ipertestuale visualizzato in Aggregato nel riquadro Dispositivi correlati della pagina Dettagli volume/integrità del volume radice SVM.
7. Individuare e fare clic sul collegamento ipertestuale visualizzato sotto Nodo nel riquadro **Dispositivi correlati** della pagina dei dettagli **Aggregato/Stato** dell'Aggregato.

La scheda Nodi nella pagina Dettagli cluster/integrità visualizza lo stato della coppia di nodi HA a cui appartiene il nodo di hosting del volume radice SVM. Lo stato del nodo è indicato sul display.

Dopo aver confermato che la condizione di offline del volume è causata dalla condizione di offline dell'SVM host di quel volume, che a sua volta è causata dal fatto che il nodo che ospita il volume radice di quell'SVM è inattivo, contattare l'amministratore o l'operatore appropriato per riavviare manualmente il nodo inattivo.

Determina se un volume è offline a causa di dischi danneggiati in un aggregato

È possibile utilizzare l'interfaccia utente Web di Unified Manager per confermare o escludere la possibilità che un volume sia offline perché problemi al disco RAID hanno portato offline il relativo aggregato host.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per determinare se la condizione di volume offline è causata da problemi del disco RAID che stanno portando offline l'aggregato di hosting, eseguire le seguenti azioni:

Passi

1. Individuare e fare clic sul collegamento ipertestuale visualizzato in Aggregato nel riquadro **Dispositivi correlati** della pagina dei dettagli **Volume/Stato**.

La pagina Dettagli aggregato/stato visualizza lo stato online o offline dell'aggregato di hosting. Se lo stato dell'aggregato è online, i problemi del disco RAID non sono la causa della disconnessione del volume.

2. Se lo stato dell'aggregato è offline, fare clic su **Informazioni disco** e cercare gli eventi di disco danneggiato nell'elenco **Eventi** nella scheda **Informazioni disco**.
3. Per identificare meglio i dischi danneggiati, fare clic sul collegamento ipertestuale visualizzato sotto Nodo nel riquadro **Dispositivi correlati**.

Viene visualizzata la pagina dei dettagli Cluster/Stato.

4. Fare clic su **Dischi**, quindi selezionare **Interrotti** nel riquadro **Filtri** per elencare tutti i dischi in stato di interruzione.

Se i dischi in stato di interruzione 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 danneggiati e dal conseguente aggregato host offline, contattare l'amministratore o l'operatore appropriato per sostituire manualmente i dischi danneggiati e rimettere online l'aggregato.

Risolvere i problemi di capacità

Questo flusso di lavoro fornisce un esempio di come è possibile risolvere un problema di capacità. In questo scenario, sei un amministratore o un operatore e accedi alla pagina Unified ManagerDashboard per verificare se uno degli oggetti di archiviazione monitorati presenta problemi di capacità. Vuoi determinare la possibile causa del problema e la sua possibile soluzione.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Nella pagina Dashboard, cercare un evento di errore "Spazio volume pieno" nel pannello Capacità sotto l'elenco a discesa degli eventi.

Passi

1. Nel pannello **Capacità** della pagina **Dashboard**, fare clic sul nome dell'evento di errore Spazio volume pieno.

Viene visualizzata la pagina dei dettagli dell'evento relativo all'errore.

2. Dalla pagina dei dettagli dell'**Evento**, puoi eseguire una o più delle seguenti attività:
 - Esaminare il messaggio di errore nel campo Causa e fare clic sui suggerimenti in Azioni correttive suggerite per esaminare le descrizioni delle possibili soluzioni.
 - Fare clic sul nome dell'oggetto, in questo caso un volume, nel campo Origine per ottenere dettagli sull'oggetto.
 - Cerca le note che potrebbero essere state aggiunte su questo evento.
 - Aggiungi una nota all'evento.
 - Assegna l'evento a un altro utente.
 - Riconosci l'evento.
 - Contrassegna l'evento come risolto.

Informazioni correlate

["Pagina dei dettagli dell'evento"](#)

Eseguire le azioni correttive suggerite per un volume completo

Dopo aver ricevuto un evento di errore “Spazio volume pieno”, puoi esaminare le azioni correttive suggerite nella pagina Dettagli evento e decidere di eseguirne una.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Un utente con qualsiasi ruolo può eseguire tutte le attività in questo flusso di lavoro che utilizzano Unified Manager.

In questo esempio, hai visualizzato un evento di errore Spazio volume pieno nella pagina dell'inventario di Unified Manager Event Management e hai fatto clic sul nome dell'evento.

Le possibili azioni correttive che potresti intraprendere per un volume intero includono quanto segue:

- Abilitazione dell'aumento automatico, della deduplicazione 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 ONTAP System Manager o da ONTAP CLI, è possibile utilizzare Unified Manager per trovare le informazioni necessarie per determinare quali azioni intraprendere.

Passi

1. Dalla 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/Integrità**, fai clic su **Configurazione** e vedrai che la deduplicazione e la

compressione sono già abilitate sul volume.

Decidi di ridimensionare il volume.

3. Nel riquadro **Dispositivi correlati**, fare clic sul nome dell'aggregato di hosting per verificare se l'aggregato può ospitare un volume maggiore.
4. Nella pagina dei dettagli **Aggregato/Stato**, puoi vedere che l'aggregato che ospita il volume completo ha sufficiente capacità non impegnata, quindi puoi utilizzare ONTAP System Manager per ridimensionare il volume, assegnandogli maggiore capacità.

Informazioni correlate

["Pagina dei dettagli dell'evento"](#)

Gestire le soglie di salute

È possibile configurare valori di soglia di integrità globali per tutti gli aggregati, i volumi e i qtree per tenere traccia di eventuali violazioni della soglia di integrità.

Quali sono le soglie di integrità della capacità di archiviazione

Una soglia di integrità della capacità di archiviazione è il punto in cui il server Unified Manager genera eventi per segnalare eventuali problemi di capacità con gli oggetti di archiviazione. È possibile configurare gli avvisi in modo che vengano inviate notifiche ogni volta che si verificano tali eventi.

Le soglie di integrità della capacità di archiviazione per tutti gli aggregati, i volumi e i qtree sono impostate sui valori predefiniti. È possibile modificare le impostazioni in base alle proprie esigenze per un oggetto o un gruppo di oggetti.

Configurare le impostazioni della soglia di salute globale

È possibile configurare le condizioni di soglia di integrità globale per capacità, crescita, riserva di snapshot, quote e inode per monitorare efficacemente le dimensioni di aggregazione, volume e qtree. È anche possibile modificare le impostazioni per la generazione di eventi in caso di superamento delle soglie di ritardo.

Le impostazioni della soglia di integrità globale si applicano a tutti gli oggetti a cui sono associate, come aggregati, volumi e così via. Quando vengono superate le soglie, viene generato un evento e, se sono configurati gli avvisi, viene inviata una notifica di avviso. I valori di soglia predefiniti sono impostati sui valori consigliati, ma è possibile modificarli per generare eventi a intervalli in base alle proprie esigenze specifiche. Quando le soglie vengono modificate, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

Le impostazioni delle soglie di salute globali sono accessibili dalla sezione Soglie evento del menu di navigazione a sinistra. È anche possibile modificare le impostazioni della soglia per singoli oggetti, dalla pagina dell'inventario o dalla pagina dei dettagli di quell'oggetto.

- Per informazioni, vedere ["Configurazione dei valori soglia di integrità aggregati globali"](#).

È possibile configurare le impostazioni della soglia di integrità per capacità, crescita e copie Snapshot per tutti gli aggregati per tenere traccia di eventuali violazioni della soglia.

- Per informazioni, vedere ["Configurazione dei valori di soglia di integrità del volume globale"](#) .

È possibile modificare le impostazioni della soglia di integrità per capacità, copie snapshot, quote qtree, crescita del volume, sovrascrittura dello spazio di riserva e inode per tutti i volumi per tenere traccia di eventuali violazioni della soglia.

- Per informazioni, vedere ["Configurazione dei valori di soglia di integrità globali di qtree"](#) .

È possibile modificare le impostazioni della soglia di integrità per la capacità di tutti i qtree per tenere traccia di qualsiasi violazione della soglia.

- Per informazioni, vedere ["Modifica delle impostazioni della soglia di integrità del ritardo per le relazioni di protezione non gestite"](#) .

È possibile aumentare o diminuire la percentuale di ritardo di avviso o di errore in modo che gli eventi vengano generati a intervalli più adatti alle proprie esigenze.

Configurare i valori soglia globali di integrità aggregata

È possibile configurare valori di soglia di integrità globali per tutti gli aggregati per monitorare qualsiasi violazione della soglia. In caso di superamento delle soglie vengono generati eventi appropriati e sulla base di questi eventi è possibile adottare misure preventive. È possibile configurare i valori globali in base alle impostazioni delle best practice per le soglie che si applicano a tutti gli aggregati monitorati.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

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 monitoraggio migliore; tuttavia, è possibile modificare i valori per adattarli ai requisiti del proprio ambiente.

Quando Autogrow è abilitato sui volumi che risiedono nell'aggregato, le soglie di capacità dell'aggregato vengono considerate superate in base alla dimensione massima del volume impostata da Autogrow, non in base alla dimensione del volume originale.



I valori di soglia di integrità non sono applicabili all'aggregato radice del nodo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Soglie evento > Aggregazione**.
2. Configurare i valori soglia appropriati per capacità, crescita e copie Snapshot.
3. Fare clic su **Salva**.

Informazioni correlate

["Aggiunta di utenti"](#)

Configurare i valori di soglia di integrità del volume globale

È possibile configurare i valori di soglia di integrità globali per tutti i volumi per tenere traccia di eventuali violazioni della soglia. In caso di superamento delle soglie di salute vengono generati eventi appropriati e, in base a questi eventi, è possibile adottare misure preventive. È possibile configurare i valori globali in base alle impostazioni delle best practice per le soglie che si applicano a tutti i volumi monitorati.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

La maggior parte delle opzioni di soglia ha valori predefiniti per un monitoraggio migliore. Tuttavia, è possibile modificare i valori per adattarli ai requisiti del proprio ambiente.

Si noti che quando Autogrow è abilitato su un volume, le soglie di capacità vengono considerate superate in base alla dimensione massima del volume impostata da Autogrow, non in base alla dimensione del volume originale.



Il valore predefinito di 1000 copie Snapshot è applicabile solo ai volumi FlexVol quando la versione ONTAP è 9.4 o successiva e ai volumi FlexGroup quando la versione ONTAP è 9.8 o successiva. 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 impostarla su un valore pari o inferiore a 250 qui, nella vista Integrità: Tutti i volumi o nella pagina dei dettagli Volume/Integrità.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Soglie eventi > Volume**.
2. Configurare i valori soglia appropriati per capacità, copie snapshot, quote qtree, crescita del volume e inode.
3. Fare clic su **Salva**.

Informazioni correlate

["Aggiunta di utenti"](#)

Configurare i valori di soglia di integrità globali di qtree

È possibile configurare i valori di soglia di integrità globali per tutti i qtree per tenere traccia di qualsiasi violazione della soglia. In caso di superamento delle soglie di salute vengono generati eventi appropriati e, in base a questi eventi, è possibile adottare misure preventive. È possibile configurare i valori globali in base alle impostazioni delle best practice per le soglie che si applicano a tutti i qtree monitorati.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Le opzioni di soglia hanno valori predefiniti per un monitoraggio migliore; tuttavia, è possibile modificare i valori per adattarli ai requisiti del proprio ambiente.

Gli eventi vengono generati per un qtree solo quando è stata impostata una quota Qtree o una quota predefinita sul qtree. Gli eventi non vengono generati se lo spazio definito in una quota utente o in una quota di gruppo ha superato la soglia.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Soglie eventi > Qtree**.
2. Configurare i valori di soglia della capacità appropriati.
3. Fare clic su **Salva**.

Configurare le impostazioni della soglia di ritardo per le relazioni di protezione non gestite

È possibile modificare le impostazioni predefinite globali relative agli avvisi di ritardo e alle soglie di errore per le relazioni di protezione non gestite, in modo che gli eventi vengano generati a intervalli appropriati alle proprie esigenze.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Il tempo di ritardo non deve essere superiore all'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 al 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Soglie evento > Relazione**.
2. Aumentare o diminuire la percentuale di tempo di ritardo predefinito per l'avviso o l'errore a livello globale, secondo necessità.
3. Per disattivare l'attivazione di un evento di avviso o errore a partire da qualsiasi soglia di ritardo, deselezionare la casella accanto a **Abilitato**.
4. Fare clic su **Salva**.

Informazioni correlate

["Aggiunta di utenti"](#)

Modifica le impostazioni delle soglie di salute aggregate individuali

È possibile modificare le impostazioni della soglia di integrità per la capacità aggregata, la crescita e le copie Snapshot di uno o più aggregati. Quando viene superata una soglia, vengono generati degli avvisi e si ricevono delle notifiche. Queste notifiche ti aiutano ad adottare misure preventive in base all'evento generato.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

In base alle modifiche ai valori soglia, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

Quando Autogrow è abilitato sui volumi che risiedono nell'aggregato, le soglie di capacità dell'aggregato vengono considerate superate in base alla dimensione massima del volume impostata da Autogrow, non in base alla dimensione del volume originale.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Nella vista **Salute: Tutti gli aggregati**, seleziona uno o più aggregati e poi fai clic su **Modifica soglie**.
3. Nella finestra di dialogo **Modifica soglie aggregate**, modificare le impostazioni della soglia di una delle seguenti: capacità, crescita o copie Snapshot selezionando la casella di controllo appropriata e quindi modificando le impostazioni.
4. Fare clic su **Salva**.

Informazioni correlate

["Aggiunta di utenti"](#)

Modifica le impostazioni della soglia di integrità del volume individuale

È possibile modificare le impostazioni della soglia di integrità per la capacità del volume, la crescita, la quota e lo spazio riservato di uno o più volumi. Quando viene superata una soglia, vengono generati degli avvisi e si ricevono delle notifiche. Queste notifiche ti aiutano ad adottare misure preventive in base all'evento generato.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

In base alle modifiche ai valori soglia, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

Si noti che quando Autogrow è abilitato su un volume, le soglie di capacità vengono considerate superate in base alla dimensione massima del volume impostata da Autogrow, non in base alla dimensione del volume originale.



Il valore predefinito di 1000 copie Snapshot è applicabile solo ai volumi FlexVol quando la versione ONTAP è 9.4 o successiva e ai volumi FlexGroup quando la versione ONTAP è 9.8 o successiva. 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 impostarla su un valore pari o inferiore a 250 qui, nella vista Integrità: Tutti i volumi o nella pagina dei dettagli Volume/Integrità.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nella vista **Integrità: Tutti i volumi**, seleziona uno o più volumi e poi fai clic su **Modifica soglie**.
3. Nella finestra di dialogo **Modifica soglie volume**, modificare le impostazioni di soglia di uno dei seguenti

elementi: capacità, copie snapshot, quota qtree, crescita o inode selezionando la casella di controllo appropriata e quindi modificando le impostazioni.

4. Fare clic su **Salva**.

Informazioni correlate

["Aggiunta di utenti"](#)

Modifica le impostazioni della soglia di integrità di qtree individuali

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 degli avvisi e si ricevono delle notifiche. Queste notifiche ti aiutano ad adottare misure preventive in base all'evento generato.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

In base alle modifiche ai valori soglia, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Qtrees**.
2. Nella vista **Capacità: Tutti i Qtree**, seleziona uno o più Qtree e poi fai clic su **Modifica soglie**.
3. Nella finestra di dialogo **Modifica soglie Qtree**, modifica le soglie di capacità per il qtree o i qtree selezionati e fai clic su **Salva**.



È anche possibile impostare singole soglie qtree dalla scheda Qtree nella pagina Dettagli VM di archiviazione/Stato.

Gestire gli obiettivi di sicurezza del cluster

Unified Manager fornisce una dashboard che identifica il livello di sicurezza dei cluster ONTAP, delle macchine virtuali di storage (SVM) e dei volumi in base alle raccomandazioni definite nella *NetApp Security Hardening Guide for ONTAP 9*.

L'obiettivo della dashboard di sicurezza è quello di mostrare tutte le aree in cui i cluster ONTAP non sono conformi alle linee guida consigliate da NetApp, in modo da poter risolvere questi potenziali problemi. Nella maggior parte dei casi è possibile risolvere i problemi utilizzando ONTAP System Manager o ONTAP CLI. La tua organizzazione potrebbe non seguire tutte le raccomandazioni, quindi in alcuni casi non sarà necessario apportare alcuna modifica.

Vedi il ["Guida al rafforzamento della sicurezza NetApp per ONTAP 9"](#) (TR-4569) per raccomandazioni e risoluzioni dettagliate.

Oltre a segnalare lo stato di sicurezza, Unified Manager genera anche eventi di sicurezza per qualsiasi cluster o SVM che presenti violazioni della sicurezza. È possibile tenere traccia di questi problemi nella pagina dell'inventario Gestione eventi e configurare avvisi per questi eventi in modo che l'amministratore dell'archiviazione venga avvisato quando si verificano nuovi eventi di sicurezza.

Per maggiori 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 alle raccomandazioni definite nella *Guida al rafforzamento della sicurezza NetApp per ONTAP 9*.

Alcuni dei controlli di sicurezza includono:

- se un cluster utilizza un metodo di autenticazione sicuro, come SAML
- se i cluster peer hanno la loro comunicazione crittografata
- se una VM di archiviazione ha il suo registro di controllo abilitato
- se i tuoi volumi hanno la crittografia software o hardware abilitata

Vedere gli argomenti sulle categorie di conformità e ["Guida al rafforzamento della sicurezza NetApp per ONTAP 9"](#) per informazioni dettagliate.



Anche gli eventi di aggiornamento segnalati dalla piattaforma Active IQ sono considerati eventi di sicurezza. Questi eventi identificano problemi per la cui risoluzione è necessario aggiornare il software ONTAP , il firmware del nodo o il software del sistema operativo (per gli avvisi di sicurezza). Questi eventi non vengono visualizzati nel pannello Sicurezza, ma sono disponibili nella pagina dell'inventario Gestione eventi.

Per maggiori informazioni, vedere ["Gestione degli obiettivi di sicurezza del cluster"](#).

Categorie di conformità del cluster

Questa tabella descrive i parametri di conformità alla sicurezza del cluster valutati da Unified Manager, la raccomandazione NetApp e se il parametro influisce sulla determinazione complessiva della conformità o meno del cluster.

La presenza di SVM non conformi su un cluster influirà sul valore di conformità del cluster. Pertanto, in alcuni casi potrebbe essere necessario risolvere un problema di sicurezza con una SVM prima che la sicurezza del cluster venga considerata conforme.

Si noti che non tutti i parametri elencati di seguito sono presenti in tutte le installazioni. Ad esempio, se non hai cluster peering o se hai disabilitato AutoSupport su un cluster, non vedrai gli elementi Cluster Peering o AutoSupport HTTPS Transport nella pagina dell'interfaccia utente.

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
FIPS globale	Indica se la modalità di conformità Global FIPS (Federal Information Processing Standard) 140-2 è abilitata o disabilitata. Quando FIPS è abilitato, TLSv1 e SSLv3 sono disabilitati e sono consentiti solo TLSv1.1 e TLSv1.2.	Abilitato	Sì
Telnet	Indica se l'accesso Telnet al sistema è abilitato o disabilitato. NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro.	Disabili	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 abilitato o disabilitato per gli utenti che accedono al sistema.	Abilitato	Sì
Cluster Peering	Indica se la comunicazione tra cluster peer è crittografata o non crittografata. Affinché questo parametro sia considerato conforme, è necessario che la crittografia sia configurata sia sul cluster di origine che su quello di destinazione.	Criptato	Sì
Protocollo di tempo di rete	Indica se il cluster ha uno o più server NTP configurati. Per garantire ridondanza e un servizio ottimale, NetApp consiglia di associare almeno tre server NTP al cluster.	Configurato	Sì

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
OCSP	A partire dalla versione 9.14.1, Active IQ Unified Manager fornisce informazioni sullo stato del protocollo OCSP (Online Certificate Status Protocol) a livello di macchina virtuale di archiviazione (SVM, precedentemente nota come Vserver). Ciò significa che la convalida OCSP viene applicata a tutte le connessioni SSL/TLS effettuate all'SVM e garantisce l'integrità e la validità dei certificati utilizzati in queste connessioni.	Abilitato	NO
Registrazione di audit remoto	Indica se l'inoltro del registro (Syslog) è crittografato o meno.	Criptato	Sì
AutoSupport del trasporto HTTPS	Indica se HTTPS viene utilizzato come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp .	Abilitato	Sì
Utente amministratore predefinito	Indica se l'utente amministratore predefinito (integrato) è abilitato o disabilitato. NetApp consiglia di bloccare (disabilitare) tutti gli account integrati non necessari.	Disabili	Sì
Utenti SAML	Indica se SAML è configurato. SAML consente di configurare l'autenticazione a più fattori (MFA) come metodo di accesso per l'accesso singolo.	NO	NO

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
Utenti di Active Directory	Indica se Active Directory è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti dagli utenti che accedono ai cluster.	NO	NO
Utenti LDAP	Indica se LDAP è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti dagli utenti che gestiscono cluster rispetto agli 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 accedere al cluster.	NO	NO
Shell remota	Indica se RSH è abilitato. Per motivi di sicurezza, RSH dovrebbe essere disattivato. Per l'accesso remoto sicuro è preferibile utilizzare Secure Shell (SSH).	Disabili	Sì
MD5 in uso	Indica se gli account utente ONTAP utilizzano la funzione hash MD5 meno sicura. È preferibile la migrazione degli account utente con hash MD5 alla funzione hash crittografica più sicura come SHA-512.	NO	Sì
Tipo di emittente del certificato	Indica il tipo di certificato digitale utilizzato.	Firmato CA	NO

Categorie di conformità delle VM di archiviazione

Questa tabella descrive i criteri di conformità alla sicurezza della macchina virtuale di archiviazione (SVM) valutati da Unified Manager, la raccomandazione NetApp e se il parametro influisce sulla determinazione complessiva della conformità o meno della SVM.

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità SVM
Registro di controllo	Indica se la registrazione di controllo è abilitata o disabilitata.	Abilitato	Sì
Impostazioni SSH non sicure	Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con <code>cbc*</code> .	NO	Sì
Banner di accesso	Indica se il banner di accesso è abilitato o disabilitato per gli utenti che accedono alle SVM sul sistema.	Abilitato	Sì
Crittografia LDAP	Indica se la crittografia LDAP è abilitata o disabilitata.	Abilitato	NO
Autenticazione NTLM	Indica se l'autenticazione NTLM è abilitata o disabilitata.	Abilitato	NO
Firma del payload LDAP	Indica se la firma del payload LDAP è abilitata o disabilitata.	Abilitato	NO
Impostazioni CHAP	Indica se CHAP è abilitato o disabilitato.	Abilitato	NO
Kerberos V5	Indica se l'autenticazione Kerberos V5 è abilitata o disabilitata.	Abilitato	NO
Autenticazione NIS	Indica se è configurato l'uso dell'autenticazione NIS.	Disabili	NO

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità SVM
Stato FPolicy Attivo	Indica se FPolicy è stato creato o meno.	Sì	NO
Crittografia SMB abilitata	Indica se la firma e la sigillatura SMB non sono abilitate.	Sì	NO
Firma SMB abilitata	Indica se la firma SMB non è abilitata.	Sì	NO

Categorie di conformità del volume

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 sulla conformità del cluster o della VM di archiviazione.

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).
Software e hardware crittografati	Visualizza il numero di volumi protetti tramite crittografia software e hardware.
Non crittografato	Visualizza il numero di volumi non crittografati.

Cosa significa non conforme

I cluster e le macchine virtuali di storage (SVM) sono considerati non conformi quando non viene soddisfatto uno qualsiasi dei criteri di sicurezza valutati in base alle raccomandazioni definite nella *NetApp Security Hardening Guide for ONTAP 9*. Inoltre, un cluster è considerato non conforme quando una qualsiasi 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 è configurato come consigliato.

-  - Il parametro non è configurato come consigliato.
-  - La funzionalità non è abilitata sul cluster oppure il parametro non è configurato come consigliato, ma questo parametro non contribuisce alla conformità dell'oggetto.

Si noti che lo stato di crittografia del volume non influisce sulla conformità del cluster o dell'SVM.

Visualizza lo stato di sicurezza per cluster e VM di archiviazione

Active IQ Unified Manager consente di visualizzare lo stato di sicurezza degli oggetti di archiviazione nel proprio 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 non autorizzate del sistema sui cluster monitorati e sulle VM di archiviazione.

Per le raccomandazioni di sicurezza, vedere il ["Guida al rafforzamento della sicurezza NetApp per ONTAP 9"](#)

Visualizza lo stato di sicurezza a livello di oggetto nella pagina Sicurezza

In qualità di amministratore di sistema, puoi utilizzare la pagina **Sicurezza** per ottenere visibilità sul livello di sicurezza dei tuoi cluster ONTAP e delle VM di storage a livello di data center e sito. Gli oggetti supportati sono cluster, VM di archiviazione e volumi. Segui questi passaggi:

Passi

1. Nel riquadro di navigazione a 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** oppure selezionare un singolo cluster dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Sicurezza**. Viene visualizzata la pagina Sicurezza.

Facendo clic sui grafici a barre, conteggi e **View Reports** i collegamenti ti portano alla pagina Volumi, Cluster o VM di archiviazione per visualizzare i dettagli corrispondenti o generare report, a seconda delle necessità.

La pagina Sicurezza visualizza i seguenti pannelli:

- **Conformità del cluster:** lo stato di sicurezza (numero di cluster conformi o non conformi) di tutti i cluster in un data center
- **Conformità delle VM di archiviazione:** lo stato di sicurezza (numero di VM di archiviazione conformi o non conformi) per tutte le VM di archiviazione nel tuo data center
- **Crittografia del volume:** lo stato di crittografia del volume (numero di volumi crittografati o non crittografati) di tutti i volumi nel tuo ambiente
- **Stato anti-ransomware del volume:** lo stato di sicurezza (numero di volumi con anti-ransomware abilitato o disabilitato) di tutti i volumi nel tuo ambiente
- **Autenticazione cluster e certificati:** il numero di cluster che utilizzano ciascun tipo di metodo di autenticazione, ad esempio SAML, Active Directory o tramite certificati e autenticazione locale. Il pannello mostra anche il numero di cluster i cui certificati sono scaduti o scadranno entro 60 giorni.

Visualizza i dettagli di sicurezza di tutti i cluster nella pagina Cluster

La pagina dei dettagli **Cluster / Sicurezza** consente di visualizzare lo stato di conformità della sicurezza a livello di cluster.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.
2. Selezionare **Visualizza > Sicurezza > Tutti i cluster**.

Vengono visualizzati i parametri di sicurezza predefiniti, quali Global FIPS, Telnet, impostazioni SSH non sicure, banner di accesso, protocollo di tempo di rete, AutoSupport HTTPS Transport e lo stato di scadenza del certificato del cluster.

Puoi cliccare su  pulsante Altre opzioni e scegliere di visualizzare i dettagli di sicurezza nella pagina **Sicurezza** di Unified Manager o in System Manager. Per visualizzare i dettagli su System Manager è necessario disporre di credenziali valide.



Se un cluster ha un certificato scaduto, puoi fare clic `expired` in **Validità del certificato cluster** e rinnovarlo da System Manager (9.10.1 e versioni successive). Non puoi cliccare `expired` se l'istanza di System Manager è di una versione precedente alla 9.10.1.

Visualizza i dettagli di sicurezza di tutti i cluster dalla pagina delle VM di archiviazione

La pagina dei dettagli **VM di archiviazione / Sicurezza** consente di visualizzare lo stato di conformità della sicurezza a livello di VM di archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Selezionare **Visualizza > Sicurezza > Tutte le VM di archiviazione**. Viene visualizzato un elenco di cluster con i parametri di sicurezza.

È possibile avere una visualizzazione predefinita della conformità di sicurezza delle VM di archiviazione controllando i parametri di sicurezza, come VM di archiviazione, cluster, banner di accesso, registro di controllo e impostazioni SSH non sicure.

Puoi cliccare su  pulsante Altre opzioni e scegliere di visualizzare i dettagli di sicurezza nella pagina **Sicurezza** di Unified Manager o in System Manager. Per visualizzare i dettagli su System Manager è necessario disporre di credenziali valide.

Per i dettagli sulla sicurezza anti-ransomware per volumi e VM di archiviazione, vedere ["Visualizzazione dello stato anti-ransomware di tutti i volumi e delle VM di archiviazione"](#).

Visualizza gli eventi di sicurezza che potrebbero richiedere aggiornamenti software o firmware

Ci sono alcuni eventi di sicurezza che hanno un'area di impatto di "Aggiornamento". Questi eventi vengono segnalati dalla piattaforma Active IQ e identificano problemi per la cui risoluzione è necessario aggiornare il software ONTAP, il firmware del nodo o il software del sistema operativo (per gli avvisi di sicurezza).

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per alcuni di questi problemi potrebbe essere necessario intervenire immediatamente, mentre per altri potrebbe essere necessario attendere la successiva manutenzione programmata. È possibile visualizzare tutti questi eventi e assegnarli agli utenti in grado di risolvere i problemi. Inoltre, se ci sono determinati eventi di aggiornamento della sicurezza di cui non vuoi essere informato, questo elenco può aiutarti a identificare tali

eventi in modo da poterli disabilitare.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.

Per impostazione predefinita, tutti gli eventi attivi (nuovi e riconosciuti) vengono visualizzati nella pagina dell'inventario Gestione eventi.

2. Dal menu Visualizza, seleziona **Aggiorna eventi**.

La pagina visualizza tutti gli eventi di sicurezza di aggiornamento attivi.

Visualizza come viene gestita l'autenticazione utente su tutti i cluster

Nella pagina Sicurezza vengono visualizzati i tipi di autenticazione utilizzati per autenticare gli utenti su ciascun cluster e il numero di utenti che accedono al cluster utilizzando ciascun tipo. Ciò consente di verificare che l'autenticazione dell'utente venga eseguita in modo sicuro, come definito dalla propria organizzazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Dashboard**.
2. Nella parte superiore della dashboard, seleziona **Tutti i cluster** dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Sicurezza** per visualizzare la pagina **Sicurezza**.
4. Visualizza la scheda **Autenticazione cluster** per vedere il numero di utenti che accedono al sistema utilizzando ciascun tipo di autenticazione.
5. Visualizzare la scheda **Sicurezza cluster** 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 un metodo non consigliato da NetApp, è possibile disabilitare il metodo.

Visualizza lo stato di crittografia di tutti i volumi

È possibile visualizzare un elenco di tutti i volumi e del loro stato di crittografia attuale, in modo da poter determinare se i dati sui volumi sono adeguatamente protetti dall'accesso da parte di utenti non autorizzati.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

I tipi di crittografia che possono essere applicati 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 tramite crittografia software e hardware.
- Nessuno: volumi non crittografati.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Salute > Crittografia volumi**
3. Nella vista **Integrità: Crittografia volumi**, ordinare in base al campo **Tipo di crittografia** oppure utilizzare il filtro per visualizzare i volumi che hanno un tipo di crittografia specifico o che non sono crittografati (Tipo di crittografia "Nessuno").

Visualizzazione dello stato anti-ransomware di tutti i volumi e delle VM di archiviazione

È possibile visualizzare un elenco di tutti i volumi e delle VM di archiviazione (SVM) e del loro stato anti-ransomware attuale, in modo da poter determinare se i dati sui volumi e sulle SVM sono adeguatamente protetti dagli attacchi ransomware.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per ulteriori informazioni sui diversi stati anti-ransomware, vedere ["ONTAP: Abilita anti-ransomware"](#).

Visualizza i dettagli di sicurezza di tutti i volumi con rilevamento anti-ransomware

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Salute > Sicurezza > Anti-ransomware**
3. Nella vista **Sicurezza: Anti-ransomware**, è possibile ordinare in base ai vari campi oppure utilizzare il Filtro.



L'anti-ransomware non è supportato per volumi offline, volumi con restrizioni, volumi SnapLock, volumi FlexGroup, volumi FlexCache, volumi solo SAN, volumi di VM di storage arrestate, volumi root di VM di storage o volumi di protezione dati.

Visualizza i dettagli di sicurezza di tutte le VM di archiviazione con rilevamento anti-ransomware

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Selezionare **Visualizza > Sicurezza > Anti-ransomware**. Viene visualizzato un elenco di SVM con stato anti-ransomware.



Il monitoraggio anti-ransomware non è supportato sulle VM di archiviazione che non hanno il protocollo NAS abilitato.

Visualizza tutti gli eventi di sicurezza attivi

È possibile visualizzare tutti gli eventi di sicurezza attivi e quindi assegnare ciascuno di essi a un utente in grado di risolvere il problema. Inoltre, se ci sono determinati eventi di sicurezza che non desideri ricevere, questo elenco può aiutarti a identificare gli eventi che vuoi disabilitare.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.

Per impostazione predefinita, gli eventi Nuovi e Riconosciuti vengono visualizzati nella pagina dell'inventario Gestione eventi.

2. Dal menu Visualizza, seleziona **Eventi di sicurezza attivi**.

La pagina visualizza tutti gli eventi di sicurezza nuovi e riconosciuti generati negli ultimi 7 giorni.

Aggiungi avvisi per eventi di sicurezza

È possibile configurare avvisi per singoli eventi di sicurezza, proprio come per qualsiasi altro evento ricevuto da Unified Manager. Inoltre, se vuoi trattare tutti gli eventi di sicurezza allo stesso modo e inviare le email alla stessa persona, puoi creare un singolo avviso per essere avvisato quando vengono attivati eventi di sicurezza.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

L'esempio seguente mostra come creare un avviso per l'evento di sicurezza "Protocollo Telnet abilitato". Verrà inviato un avviso se l'accesso Telnet è configurato per l'accesso amministrativo remoto al cluster. È possibile utilizzare la stessa metodologia per creare avvisi per tutti gli eventi di sicurezza.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
2. Nella pagina **Impostazione avviso**, fare clic su **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 il cluster o i cluster su cui si desidera abilitare questo avviso.
5. Fare clic su **Eventi** ed eseguire le seguenti azioni:
 - a. Nell'elenco Gravità evento, selezionare **Avviso**.
 - b. Nell'elenco Eventi corrispondenti, selezionare **Protocollo Telnet abilitato**.
6. Fare clic su **Azioni** e quindi selezionare il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
7. Configurare qualsiasi altra opzione in questa pagina per la frequenza delle notifiche, l'emissione di trap SNMP e l'esecuzione di uno script.
8. Fare clic su **Salva**.

Disabilitare eventi di sicurezza specifici

Tutti gli eventi sono abilitati per impostazione predefinita. È possibile disabilitare eventi specifici per impedire la generazione di notifiche per quegli eventi che non sono importanti nel proprio ambiente. È possibile abilitare gli eventi disabilitati se si desidera riprendere a ricevere le relative notifiche.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Quando si disabilitano gli eventi, gli eventi generati in precedenza nel sistema vengono contrassegnati come obsoleti e gli avvisi configurati per tali eventi non vengono attivati. Quando si abilitano eventi disabilitati, le notifiche per questi eventi vengono generate a partire dal ciclo di monitoraggio successivo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione evento**.
2. Nella pagina Impostazione **Evento**, disabilita o abilita gli eventi scegliendo una delle seguenti opzioni:

Se lo desidera...	Allora fai così...
Disabilitare gli eventi	a. Fare clic su Disabilita. b. Nella finestra di dialogo Disabilita eventi, selezionare la gravità Avviso. Questa è la categoria per tutti gli eventi di sicurezza. c. Nella colonna Eventi corrispondenti, seleziona gli eventi di sicurezza che desideri disabilitare, quindi fai clic sulla freccia destra per spostare tali eventi nella colonna Disabilita eventi. d. Fare clic su Salva e chiudi. e. Verificare che gli eventi disabilitati siano visualizzati nella vista elenco della pagina Impostazione evento.
Abilita eventi	a. Dall'elenco degli eventi disabilitati, seleziona la casella di controllo relativa all'evento o agli eventi che desideri riabilitare. b. Fare clic su Abilita.

Eventi di sicurezza

Gli eventi di sicurezza forniscono informazioni sullo stato di sicurezza dei cluster ONTAP, delle macchine virtuali di archiviazione (SVM) e dei volumi in base ai parametri definiti nella *NetApp Security Hardening Guide for ONTAP 9*. Questi eventi ti avvisano di potenziali problemi, in modo che tu possa valutarne la gravità e, se necessario, risolverli.

Gli eventi di sicurezza sono raggruppati in base al tipo di origine e includono il nome dell'evento e della trappola, il livello di impatto e la gravità. Questi eventi vengono visualizzati nelle categorie di eventi VM cluster e storage.

Gestire le operazioni di backup e ripristino

È possibile creare backup di Active IQ Unified Manager e utilizzare la funzionalità di ripristino per ripristinare il backup sullo stesso sistema (locale) o su un nuovo sistema (remoto) in caso di errore del sistema o perdita di dati.

Sono disponibili tre metodi di backup e ripristino, a seconda del sistema operativo su cui è installato Unified Manager e in base al numero di cluster e nodi gestiti:

Sistema operativo	Dimensione della distribuzione	Metodo di backup consigliato
VMware vSphere	Qualunque	Snapshot VMware dell'appliance virtuale Unified Manager
Red Hat Enterprise Linux	Piccolo	Dump del database MySQL di Unified Manager
	Grande	Snapshot NetApp del database Unified Manager
Microsoft Windows	Piccolo	Dump del database MySQL di Unified Manager
	Grande	Snapshot NetApp del database Unified Manager con protocollo iSCSI

Questi diversi metodi sono descritti nelle sezioni seguenti.

Backup e ripristino per Unified Manager su appliance virtuale

Il modello di backup e ripristino per Unified Manager, quando installato su un'appliance virtuale, consiste nell'acquisire e ripristinare un'immagine dell'intera applicazione virtuale.

Le seguenti attività consentono di completare un backup dell'appliance virtuale:

1. Spegnerne la macchina virtuale ed eseguire uno snapshot VMware dell'appliance virtuale Unified Manager.
2. Creare una copia di NetApp Snapshot sul datastore per acquisire lo snapshot VMware.

Se il datastore non è ospitato su un sistema che esegue il software ONTAP , seguire le linee guida del fornitore di storage per creare un backup dello snapshot VMware.

3. Replicare la copia dello snapshot NetApp , o l'equivalente dello snapshot, su un archivio 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 VM, puoi utilizzare lo snapshot VMware creato per ripristinare la VM allo stato di backup point-in-time.

Backup e ripristino tramite dump del database MySQL

Un backup dump del database MySQL è una copia del database e dei file di configurazione Active IQ Unified Manager che è possibile utilizzare in caso di errore del sistema o perdita di dati. È possibile pianificare la scrittura di un backup su una

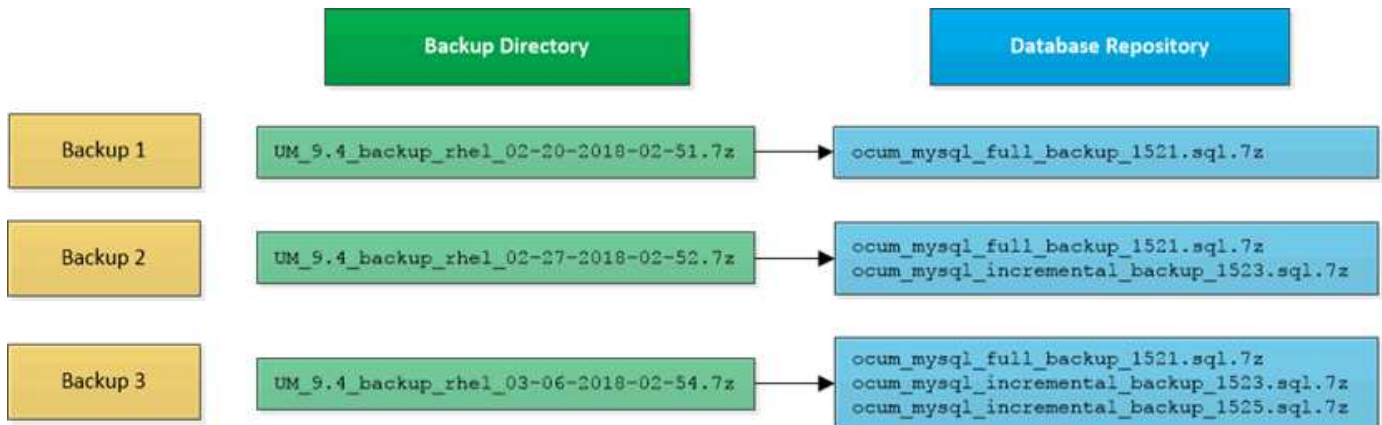
destinazione locale o su una destinazione remota. Si consiglia vivamente di definire una posizione remota esterna al sistema host Active IQ Unified Manager .



Il dump del database MySQL è il meccanismo di backup predefinito quando Unified Manager è installato su un server Linux e Windows. Tuttavia, se Unified Manager gestisce un numero elevato di cluster e nodi, o se i backup di MySQL richiedono molte ore per essere completati, è possibile eseguire il backup utilizzando copie Snapshot. Questa funzionalità è disponibile su Red Hat Enterprise Linux e Windows.

Un backup 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 presenti 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 un file di backup completo nella directory del repository del database. La volta successiva che si genera un backup, viene creato un singolo file nella directory di backup e un file di backup incrementale nella directory del repository del database che contiene le differenze rispetto al file di backup completo. Questo processo continua man mano che si creano backup aggiuntivi, fino al raggiungimento dell'impostazione di conservazione massima, come mostrato nella figura seguente.



Non rinominare o rimuovere nessuno dei file di backup in queste due directory, altrimenti qualsiasi operazione di ripristino successiva non riuscirà.

Se si scrivono i file di backup sul sistema locale, è necessario avviare un processo per copiare i file di backup in una posizione remota, in modo che siano disponibili nel caso in cui si verifichi un problema di sistema che richieda 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 e le directory di backup richiesti esistano e siano scrivibili. Controlla anche che ci sia abbastanza spazio sul sistema per creare il file di backup.

Configurare la destinazione e la pianificazione per i backup del 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 conteggio della conservazione e la pianificazione del backup. È possibile abilitare backup programmati giornalieri o settimanali. Per impostazione predefinita, i backup pianificati sono disabilitati, ma è consigliabile impostare una pianificazione di backup.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario disporre di almeno 150 GB di spazio disponibile nella posizione definita come percorso di backup.

Si consiglia di utilizzare una posizione remota esterna al sistema host di Unified Manager.

- Quando Unified Manager è installato su un sistema Linux e si utilizza il backup MySQL, assicurarsi che le seguenti autorizzazioni e proprietà siano impostate sulla directory di backup.

Permessi: 0750, Proprietà: jboss:maintenance

- Quando Unified Manager è 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 si esegue un backup è necessario più tempo rispetto ai backup successivi, perché il primo backup è un backup completo. Un backup completo può superare 1 GB e durare dalle tre alle quattro ore. I backup successivi sono incrementali e richiedono meno tempo.



- Se il numero di file di backup incrementali è troppo grande per lo spazio allocato per i backup, è possibile eseguire periodicamente un backup completo per sostituire il vecchio backup e i relativi file incrementali. In alternativa, è possibile effettuare un backup utilizzando le copie Snapshot.
- Il backup effettuato durante i primi 15 giorni di aggiunta di un nuovo cluster potrebbe non essere sufficientemente accurato per ottenere i dati storici sulle prestazioni.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Backup del database**.
2. Nella pagina **Backup del database**, fare clic su **Impostazioni di backup**.
3. Configurare i valori appropriati per un percorso di backup, un conteggio di conservazione e una pianificazione.

Il valore predefinito per il conteggio della conservazione è 10; è possibile utilizzare 0 per creare backup illimitati.

4. Selezionare il pulsante **Pianificato quotidianamente** o **Pianificato settimanalmente**, quindi specificare i dettagli della pianificazione.
5. Fare clic su **Applica**.

I file di backup del dump del database vengono creati in base alla pianificazione. È possibile visualizzare i file di backup disponibili nella pagina Backup del database.

Che cosa è un ripristino del database

Il ripristino del database MySQL è il processo di ripristino di un file di backup di Unified Manager esistente sullo stesso server Unified Manager o su uno diverso. 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 tutti i file di backup sono archiviati localmente, è possibile eseguire l'opzione di ripristino utilizzando la posizione predefinita. Se si esegue

un'operazione di ripristino su un sistema Unified Manager diverso (un sistema remoto), è necessario copiare il file o i file di backup dall'archivio secondario al disco locale prima di eseguire l'opzione di ripristino.

Durante il processo di ripristino, verrai disconnesso da Unified Manager. Una volta completato il processo di ripristino, sarà possibile accedere al sistema.

Se si ripristina l'immagine di backup su un nuovo server, al termine dell'operazione di ripristino è necessario generare un nuovo certificato di sicurezza HTTPS e riavviare il server Unified Manager. Sarà inoltre necessario riconfigurare le impostazioni di autenticazione SAML, se necessario, quando si ripristina l'immagine di backup su un nuovo server.



Non è possibile utilizzare i vecchi file di backup 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 sicurezza HTTPS"](#)

["Abilitazione dell'autenticazione SAML"](#)

["Autenticazione con Active Directory o OpenLDAP"](#)

Ripristinare un backup del database MySQL su Windows

In caso di perdita o danneggiamento dei dati, è possibile utilizzare la funzionalità di ripristino per riportare 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 remoto utilizzando la console di manutenzione di Unified Manager.

Prima di iniziare

- 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 nel `\database_dumps_repo` sottodirectory sotto il `\backup` elenco.

- 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, mentre 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 il percorso relativo del file di backup tra virgolette doppie.

Passi

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. Accedi al sistema Unified Manager con le credenziali di amministratore.
3. Avvia PowerShell o il prompt dei comandi come amministratore di Windows.
4. Inserisci il comando `maintenance_console` e premere Invio.
5. Nel **Menu principale** della console di manutenzione, immettere il numero per l'opzione **Backup e ripristino**.
6. Immettere il numero per il **Ripristino backup 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_backup_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, procedere come segue:

1. Sul server Workflow Automation, modificare l'indirizzo IP del server Unified Manager in modo che punti alla macchina più recente.
2. Sul server Unified Manager, reimpostare la password del database se l'acquisizione non riesce nel passaggio 1.

Backup e ripristino tramite NetApp Snapshots

Una copia Snapshot NetApp crea un'immagine puntuale del database e dei file di configurazione di Unified Manager che è possibile utilizzare per il ripristino in caso di errore del sistema o perdita di dati. È possibile pianificare periodicamente la scrittura di una copia Snapshot su un volume di uno dei cluster ONTAP, in modo da avere sempre una copia aggiornata.



Questa funzionalità non è disponibile per Active IQ Unified Manager installato su un'appliance virtuale.

Configurare il backup su Linux

Se Active IQ Unified Manager è installato su un computer 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, quindi l'interruzione dell'installazione è minima. L'immagine occupa uno spazio di archiviazione minimo e comporta un sovraccarico di prestazioni trascurabile, poiché registra solo le modifiche apportate ai file dall'ultima copia Snapshot effettuata. Poiché lo 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 di 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 hai creato un backup su Unified Manager 9.16, il backup può essere ripristinato solo sui sistemi Unified Manager 9.16.

- Se si apportano modifiche alla configurazione dello snapshot, lo snapshot potrebbe non essere più valido.

Configurare la posizione della copia dello snapshot

È possibile configurare il volume in cui verranno archiviate le copie Snapshot su uno dei cluster ONTAP utilizzando ONTAP System Manager o ONTAP CLI.

Prima di iniziare

Il cluster, la VM di archiviazione e il volume devono soddisfare i seguenti requisiti:

- Requisiti del cluster:
 - È necessario installare ONTAP 9.3 o versione successiva
 - Dovrebbe essere geograficamente vicino al server Unified Manager
 - Può essere monitorato da Unified Manager, ma non è obbligatorio
- Requisiti della VM di archiviazione:
 - Il cambio nome e la mappatura dei nomi devono essere impostati per utilizzare “files”
 - Utenti locali creati per corrispondere con gli utenti lato client
 - Assicurati che sia selezionato l'accesso in lettura/scrittura completo
 - Assicurati che l'accesso Superuser sia impostato su “any” nella policy di esportazione
 - NFS per NetApp Snapshot per Linux
 - NFSv4 deve essere abilitato sul server NFS e sul dominio ID NFSv4 specificato sul client e sulla VM di archiviazione
 - Il volume dovrebbe essere almeno il doppio della dimensione della directory Unified Manager/opt/netapp/data

Utilizzare il comando `du -sh /opt/netapp/data/` per verificare la dimensione corrente.

- Requisiti di volume:
 - Il volume dovrebbe essere almeno il doppio della dimensione della directory /opt/netapp/data di Unified Manager
 - Lo stile di sicurezza deve essere impostato su UNIX
 - Il criterio di snapshot locale deve essere disabilitato
 - Il dimensionamento automatico del volume dovrebbe essere abilitato
 - Il livello di servizio delle prestazioni dovrebbe essere impostato su una politica con IOPS elevati e bassa latenza, ad esempio “Extreme”

Per i passaggi dettagliati per creare il volume NFS, vedere ["Come configurare NFSv4 in ONTAP 9"](#) e il ["Guida](#)

Specificare la posizione di destinazione per le copie Snapshot

È necessario configurare la posizione di destinazione per le copie di Active IQ Unified Manager Snapshot su un volume già configurato in uno dei cluster ONTAP . Per definire la posizione è necessario utilizzare la console di manutenzione.

- È necessario disporre delle credenziali 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 gestione del cluster, del nome della VM di archiviazione, del nome del volume e del nome utente e della password del sistema di archiviazione.
- È necessario aver montato il volume sull'host Active IQ Unified Manager e disporre del percorso di montaggio.

Passi

1. Utilizzare Secure Shell per connettersi all'indirizzo IP o al nome di dominio completo del sistema Active IQ Unified Manager .
2. Accedi al sistema con il nome utente di manutenzione (umadmin) e la password.
3. Inserisci il comando `maintenance_console` e premere Invio.
4. Nel **Menu principale** della console di manutenzione, immettere il numero per l'opzione **Backup e ripristino**.
5. Immettere il numero per **Configura NetApp Snapshot Backup**.
6. Immettere il numero per configurare NFS.
7. Rivedi le informazioni che dovrai fornire e poi inserisci il numero per **Inserisci i dettagli della configurazione di backup**.
8. Per identificare il volume in cui verrà scritto lo snapshot, immettere l'indirizzo IP dell'interfaccia di gestione del cluster, il nome della VM di archiviazione, il nome del volume, il nome LUN, il nome utente e la password del sistema di archiviazione e il percorso di montaggio.
9. Verifica queste informazioni e inserisci `y` .

Il sistema esegue le seguenti attività:

- Stabilisce la connessione al cluster
 - Arresta 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 Active IQ Unified Manager per creare una pianificazione per la copia Snapshot, se non lo si è già fatto.

Configurare il backup su Windows

Active IQ Unified Manager supporta il backup e il ripristino tramite NetApp Snapshot sul sistema operativo Windows con l'ausilio di LUN tramite protocollo iSCSI.

È possibile eseguire il backup basato su snapshot mentre tutti i servizi di Unified Manager sono in esecuzione. Uno stato coerente del database viene acquisito come parte dello Snapshot, poiché il backup applica un blocco di lettura globale all'intero database, impedendo qualsiasi scrittura simultanea. Per consentire al sistema Unified Manager installato sul sistema operativo Windows di eseguire il backup e il ripristino tramite NetApp Snapshot, è necessario innanzitutto configurare il backup di Unified Manager basato su Snapshot tramite la 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 la macchina host Windows

Configurare la posizione di backup per Windows

Dopo aver eseguito il backup di Unified Manager su Windows, è necessario configurare il volume per l'archiviazione delle copie Snapshot.

Prima di iniziare

Il cluster, la VM di archiviazione e il volume devono soddisfare i seguenti requisiti:

- Requisiti del cluster:
 - È necessario installare ONTAP 9.3 o versione successiva
 - Dovrebbe essere geograficamente vicino al server Unified Manager
 - È monitorato da Unified Manager
- Requisiti della VM di archiviazione:
 - Connettività iSCSI sul cluster ONTAP
 - Il protocollo iSCSI deve essere abilitato per la macchina configurata
 - Dovresti avere un volume e una LUN dedicati per la configurazione del backup. Il volume selezionato deve contenere solo una LUN e nient'altro.
 - La dimensione del LUN deve essere almeno il doppio della dimensione dei dati che si prevede di gestire in Active IQ Unified Manager 9.9.

Ciò stabilisce anche lo stesso requisito di dimensione per il volume.
 - Assicurati che sia selezionato l'accesso in lettura/scrittura completo
 - Assicurati che l'accesso Superuser sia impostato su "any" nella policy di esportazione
- Requisiti di volume e LUN:
 - Il volume deve essere almeno il doppio della dimensione della directory dati MySQL di Unified Manager.
 - Lo stile di sicurezza deve essere impostato su Windows
 - Il criterio di snapshot locale deve essere disabilitato

- Il dimensionamento automatico del volume dovrebbe essere abilitato
- Il livello di servizio delle prestazioni dovrebbe essere impostato su una politica con IOPS elevati e bassa latenza, ad esempio “Extreme”

Configurare il cluster ONTAP

È necessario eseguire alcuni passaggi di preconfigurazione sui cluster ONTAP prima di poter eseguire il backup e il ripristino Active IQ Unified Manager utilizzando la copia Snapshot sui sistemi Windows.

È possibile configurare il cluster ONTAP utilizzando il prompt dei comandi o l'interfaccia utente di System Manager. La configurazione del cluster ONTAP prevede la configurazione dei LIF dati in modo che siano disponibili per essere assegnati come LIF iSCSI alla VM di archiviazione. Il passaggio successivo consiste nel configurare una VM di archiviazione abilitata per iSCSI utilizzando l'interfaccia utente di System Manager. Sarà necessario configurare un percorso di rete statico per questa VM di archiviazione per controllare il modo in cui i LIF utilizzano la rete per il traffico in uscita.



Dovresti avere un volume dedicato e un LUN per la configurazione del backup. Il volume selezionato deve includere una sola LUN. La dimensione del LUN deve essere almeno il doppio della dimensione dei dati che si prevede vengano gestiti da Active IQ Unified Manager.

È necessario eseguire la seguente configurazione:

Passi

1. Configurare una VM di archiviazione abilitata per iSCSI oppure utilizzare una VM di archiviazione esistente con la stessa configurazione.
2. Configurare un percorso di rete per la VM di archiviazione configurata.
3. Configurare un volume di capacità adeguata e un singolo LUN al suo interno, assicurandosi che il volume sia dedicato solo a questo LUN.



In uno scenario in cui il LUN viene creato su System Manager, l'annullamento della mappatura del LUN potrebbe eliminare l'igroup e il ripristino potrebbe non riuscire. Per evitare questo scenario, assicurarsi che durante la creazione di un LUN, questo venga creato in modo esplicito e non venga eliminato quando il LUN non è più mappato.

4. Configurare un gruppo di iniziatori nella VM di archiviazione.
5. Configurare un set di porte.
6. Integrare l'igroup con il portset.
7. Mappare il LUN sull'igroup.

Configurare la macchina host Windows

È necessario configurare il computer host Windows prima di poter utilizzare NetApp Snapshot per eseguire il backup e il ripristino Active IQ Unified Manager. Per avviare l'iniziatore iSCSI Microsoft su un computer host Windows, digitare “iscsi” nella barra di ricerca e fare clic su **iSCSI Initiator**.

Prima di iniziare

Dovresti ripulire tutte le configurazioni precedenti sulla macchina host.

Se si tenta di avviare l'iniziatore iSCSI su una nuova installazione di Windows, verrà richiesta una conferma e, una volta confermata, verrà visualizzata la finestra di dialogo Proprietà iSCSI. Se si tratta di un'installazione Windows esistente, la finestra di dialogo Proprietà iSCSI viene visualizzata con una destinazione inattiva o che sta tentando di connettersi. Pertanto, sarà necessario assicurarsi che tutte le configurazioni precedenti sull'host Windows vengano rimosse.

Passi

1. Pulire tutte le configurazioni precedenti sulla macchina host.
2. Scopri il portale di destinazione.
3. Connettiti al portale di destinazione.
4. Connettersi tramite multipath al portale di destinazione.
5. Scopri entrambi i LIF.
6. Scopri il LUN configurato nel computer Windows come dispositivo.
7. Configurare il LUN rilevato come nuova unità di volume in Windows.

Specificare la posizione di destinazione per le copie Snapshot su Windows

È necessario configurare la posizione di destinazione per le copie di Active IQ Unified Manager Snapshot su un volume già configurato in uno dei cluster ONTAP . Per definire la posizione è necessario utilizzare la console di manutenzione.

- È necessario disporre dei privilegi 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 gestione del cluster, del nome della VM di archiviazione, del nome del volume, del nome LUN e del nome utente e della password del sistema di archiviazione.
- È necessario aver montato il volume come unità di rete sull'host Active IQ Unified Manager e disporre dell'unità di montaggio.

Passi

1. Utilizzando Power Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Active IQ Unified Manager .
2. Accedi al sistema con il nome utente di manutenzione (umadmin) e la password.
3. Inserisci il comando `maintenance_console` e premere Invio.
4. Nel **Menu principale** della console di manutenzione, immettere il numero per l'opzione **Backup e ripristino**.
5. Immettere il numero per **Configura NetApp Snapshot Backup**.
6. Immettere il numero per configurare iSCSI.
7. Rivedi le informazioni che dovrai fornire e poi inserisci il numero per **Inserisci i dettagli della configurazione di backup**.
8. Per identificare il volume in cui verrà scritto lo snapshot, immettere l'indirizzo IP dell'interfaccia di gestione del cluster, il nome della VM di archiviazione, il nome del volume, il nome LUN, il nome utente e la password del sistema di archiviazione e l'unità di montaggio.
9. Verifica queste informazioni e inserisci `y` .

Il sistema esegue le seguenti attività:

- La VM di archiviazione è convalidata
- Il volume è convalidato
- Monta l'unità e lo stato è convalidato
- Esistenza e stato della LUN
- Esistenza dell'unità di rete
- L'esistenza dello spazio consigliato (più del doppio della directory dati MySQL) nel volume montato è convalidata
- Percorso LUN corrispondente al LUN dedicato nel volume
- nome igroup
- GUID del volume in cui è montata l'unità di rete
- Iniziatore iSCSI 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.

Configurare il backup tramite copia Snapshot dalla console di manutenzione

Per eseguire il backup di Active IQ Unified Manager tramite la copia Snapshot, è necessario eseguire alcuni passaggi di configurazione dalla console di manutenzione.

Prima di iniziare

Dovresti avere i seguenti dettagli per il tuo sistema:

- Indirizzo IP del cluster
- Nome VM di archiviazione
- Nome del volume
- Nome LUN
- Sentiero del monte
- Credenziali del sistema di archiviazione

Passi

1. Accedi alla console di manutenzione di Unified Manager.
2. Immettere 4 per selezionare **Backup Ripristino**.
3. Immettere 2 per selezionare **Backup e ripristino tramite NetApp Snapshot**.



Se si desidera modificare la configurazione del backup, immettere 3 per selezionare *Aggiorna configurazione backup snapshot NetApp *. Puoi solo aggiornare la password.

4. Dal menu, immettere 1 per selezionare **Configura 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 confermare che la LUN è montata sull'host.

Il processo verifica quindi che la directory dei dati, il percorso LUN, la VM di archiviazione, i volumi, la

disponibilità di spazio, l'unità e così via forniti siano corretti. Le operazioni che avvengono in background sono:

- I servizi sono interrotti
- La directory del database viene spostata nello storage montato
- La directory del database viene eliminata e vengono stabiliti i collegamenti simbolici
- I servizi vengono riavviati. Dopo il completamento della configurazione nell'interfaccia di 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 dello snapshot, poiché ciò potrebbe rendere lo snapshot non valido. Supponiamo di aver configurato il backup nell'unità G e di aver creato uno snapshot. Successivamente hai riconfigurato il backup sull'unità E e i dati vengono salvati sull'unità E in base alla nuova configurazione. Se si tenta di ripristinare uno snapshot acquisito mentre si trovava nell'unità G, l'operazione fallisce e si verifica un errore che indica che l'unità G non esiste.

Definisci una pianificazione di backup per Linux e Windows

È possibile configurare la pianificazione in base alla quale vengono create le copie di Unified Manager Snapshot tramite l'interfaccia utente di Unified Manager.

Prima di iniziare

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- 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 effettuato durante i primi 15 giorni di aggiunta di un nuovo cluster potrebbe non essere sufficientemente accurato per ottenere i dati storici sulle prestazioni.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Backup del database**.
2. Nella pagina **Backup del database**, fare clic su **Impostazioni di backup**.
3. Immettere il numero massimo di copie Snapshot che si desidera conservare nel campo **Conteggio conservazione**.

Il valore predefinito per il conteggio della 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 ONTAP.

4. Selezionare il pulsante **Pianificato quotidianamente** o **Pianificato settimanalmente**, quindi specificare i dettagli della pianificazione.
5. Fare clic su **Applica**.

Le copie snapshot vengono create in base alla pianificazione. È possibile visualizzare i file di backup disponibili nella pagina Backup del database.

Data l'importanza di questo volume e degli snapshot, potresti voler 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 **Spazio volume pieno** per impostare l'avviso.

È possibile aggiungere capacità al volume utilizzando ONTAP System Manager o ONTAP CLI in modo che il database Unified Manager non esaurisca lo spazio.

- Il numero di snapshot è prossimo a raggiungere il numero massimo. Utilizzare l'evento **Troppe copie snapshot** per impostare l'avviso.

È possibile eliminare gli snapshot più vecchi utilizzando ONTAP System Manager o ONTAP CLI in modo che ci sia sempre spazio per nuove copie di snapshot.

È possibile configurare gli avvisi nella pagina Impostazione avvisi.

Ripristina Unified Manager utilizzando 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 Unified Manager Snapshot su un sistema operativo locale o remoto utilizzando la console di manutenzione di Unified Manager.

Prima di iniziare

- È necessario disporre delle credenziali utente root per l'host Linux e dei privilegi amministrativi per la macchina 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.

Passi

1. Connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager.
 - Linux: Shell sicura
 - Windows: Power Shell
2. Accedi al sistema con le credenziali dell'utente root.
3. Inserisci il comando `maintenance_console` e premere Invio.
4. Nel **Menu principale** della console di manutenzione, immettere 4 per l'opzione **Backup e ripristino**.
5. Immettere 2 per selezionare **Backup e ripristino tramite 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. Immettere 1 per selezionare **Configura NetApp Snapshot Backup** e configurare le impostazioni per le copie Snapshot così come sono sul sistema originale.

6. Immettere 3 per selezionare **Ripristina tramite NetApp Snapshot**.
7. Selezionare la copia Snapshot da cui si desidera ripristinare Unified Manager. Premere **Invio**.
8. Una volta completato il processo di ripristino, accedi all'interfaccia utente di Unified Manager.

Dopo aver ripristinato il backup, se il server Workflow Automation non funziona, procedere come segue:

1. Sul server Workflow Automation, modificare l'indirizzo IP del server Unified Manager in modo che punti alla macchina più recente.
2. Sul server Unified Manager, reimpostare la password del database se l'acquisizione non riesce nel passaggio 1.

Modificare il 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 **Annulla configurazione NetApp Snapshot Backup** consente di tornare al backup basato su MySQL.

Prima di iniziare

Per accedere alla console di manutenzione del server Unified Manager è necessario disporre di un ID utente e di una password autorizzati.

Passi

1. Accedere alla console di manutenzione.
2. Selezionare 4 dal **Menu principale** per il backup e il ripristino.
3. Selezionare 2 dal **Menu Backup e Ripristino**.
4. Selezionare 4 per **Annulla configurazione NetApp Snapshot Backup**.

Vengono visualizzate le azioni eseguite, ovvero: arrestare i servizi, interrompere il collegamento simbolico, spostare i dati dall'archivio alla directory e quindi riavviare i servizi.

Dopo aver modificato il metodo di backup, il meccanismo di backup passa dalla copia Snapshot al backup MySQL predefinito. Questa modifica appare nella sezione Backup del database delle impostazioni generali.

Backup su richiesta per Unified Manager

È possibile utilizzare l'interfaccia utente Active IQ Unified Manager per generare backup su richiesta ogni volta che è necessario. Il backup su richiesta consente di creare istantaneamente un backup utilizzando il metodo di backup esistente. Il backup su richiesta non fa distinzione tra backup basati su MySQL o NetApp Snapshot.

È possibile eseguire il backup su richiesta utilizzando il pulsante **Esegui backup ora** nella pagina Backup del database. Il backup su richiesta non dipende dalle pianificazioni configurate per Active IQ Unified Manager.

Migrare un'appliance virtuale Unified Manager su un sistema Linux

È possibile ripristinare un backup dump del database MySQL di Unified Manager da un'appliance virtuale a un sistema Red Hat Enterprise Linux se si desidera modificare il sistema operativo host su cui è in esecuzione Unified Manager.

Prima di iniziare

- Sull'appliance virtuale:

- È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario conoscere il nome dell'utente addetto alla manutenzione di Unified Manager per l'operazione di ripristino.
- Sul sistema Linux:
 - È necessario aver installato Unified Manager su un server Linux seguendo le istruzioni in ["Installazione di Unified Manager su sistemi Linux"](#).
 - La versione di Unified Manager su questo server deve essere la stessa della versione presente sull'appliance virtuale da cui si sta utilizzando 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 utente root per l'host Linux.

Questi passaggi descrivono come creare un file di backup sull'appliance virtuale, copiare i file di backup su Red Hat Enterprise Linux e quindi ripristinare il backup del database sul nuovo sistema.

Passi

1. Sull'appliance virtuale, fare clic su **Gestione > Backup del database**.
2. Nella pagina **Backup del database**, fare clic su **Impostazioni di backup**.
3. Modificare il percorso di backup in `/jail/support`.
4. Nella sezione Pianificazione, seleziona **Pianificato quotidianamente** e inserisci un orario di qualche minuto successivo all'orario corrente, in modo che il backup venga creato il prima possibile.
5. Fare clic su **Applica**.
6. Attendi qualche ora affinché il backup venga generato.

Un backup completo può avere dimensioni superiori a 1 GB e può richiedere dalle tre alle quattro ore per essere completato.

7. Accedi come utente root all'host Linux su cui è installato Unified Manager e copia 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/* .
```

Assicurati di aver copiato il file di backup `.7z` e tutti i file del repository `.7z` nella sottodirectory `/database-dumps-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. Una volta completata l'operazione di ripristino, accedi all'interfaccia utente Web di Unified Manager.

Dovresti svolgere le seguenti attività:

- Generare un nuovo certificato di sicurezza HTTPS e riavviare il server Unified Manager.

- Modificare il percorso di backup con l'impostazione predefinita per il sistema Linux (/data/ocum-backup) oppure con un nuovo percorso a scelta, poiché sul sistema Linux non esiste alcun percorso /jail/support.
- Se si utilizza WFA, riconfigurare entrambi i lati della connessione Workflow Automation.
- Se si utilizza SAML, riconfigurare le impostazioni di autenticazione SAML.

Dopo aver verificato che tutto funzioni come previsto sul sistema Linux, è possibile arrestare e rimuovere l'appliance virtuale Unified Manager.

Gestisci gli script

È possibile utilizzare gli script per modificare o aggiornare automaticamente più oggetti di archiviazione 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.

La possibilità di caricare script su Unified Manager ed eseguirli è abilitata per impostazione predefinita. Se la tua organizzazione non desidera consentire questa funzionalità per motivi di sicurezza, puoi disattivarla da

Gestione archiviazione > Impostazioni funzionalità.

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 problemi con gli oggetti di archiviazione o identificare quali oggetti di archiviazione generano gli eventi.

Quando viene generato un avviso per un evento in Unified Manager, viene inviata un'e-mail di avviso ai destinatari specificati. Se hai 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 hai creato uno script personalizzato e lo hai 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 **Correggi** non sono disponibili per impostazione predefinita nella pagina 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 sugli eventi correlati o modificare gli

oggetti di archiviazione.

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
```

Aggiungi 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 archiviazione per i quali viene generato l'evento.

Prima di iniziare

- 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
Finestre	Script PowerShell, Perl, Python e <code>.bat</code>

- Per gli script Perl, Perl deve essere installato sul server Unified Manager. Per le installazioni VMware, Perl 5 è installato per impostazione predefinita e gli script supporteranno solo ciò che Perl 5 supporta. Se Perl è stato installato dopo Unified Manager, è necessario riavviare il server Unified Manager.
- Per gli script di PowerShell, è necessario impostare sul server Windows i criteri di esecuzione di PowerShell appropriati affinché gli script possano essere eseguiti.



Se lo script crea file di registro per monitorare l'avanzamento dello script di avviso, è necessario assicurarsi che i file di registro non vengano creati in alcun punto della cartella di installazione di Unified Manager.

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile caricare script personalizzati e raccogliere dettagli sugli eventi relativi all'avviso.



Se questa funzionalità non è disponibile nell'interfaccia utente, è perché è stata disabilitata dall'amministratore. Se necessario, è possibile abilitare questa funzionalità da **Gestione archiviazione > Impostazioni funzionalità**.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Script**.
2. Nella pagina **Script**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi script**, fare clic su **Sfoglia** per selezionare il file di script.
4. Inserisci una descrizione per lo script selezionato.
5. Fare clic su **Aggiungi**.

Elimina gli script

È possibile eliminare uno script da Unified Manager quando non è più necessario o valido.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Lo script non deve essere associato a un avviso.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Script**.
2. Nella pagina **Script**, seleziona lo script che vuoi eliminare, quindi fai clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Esecuzione dello script di test

È possibile verificare che lo script venga eseguito correttamente quando viene generato un avviso per un oggetto di archiviazione.

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver caricato uno script nel formato di file supportato su Unified Manager.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Script**.
2. Nella pagina **Script**, aggiungi lo script di prova.
3. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Configurazione avvisi**.
4. Nella pagina **Impostazione avviso**, eseguire una delle seguenti azioni:

A...	Fai questo...
Aggiungi un avviso	a. Fare clic su Aggiungi. b. Nella sezione Azioni, associa l'avviso allo script di test.

A...	Fai questo...
Modifica un avviso	a. Seleziona un avviso, quindi fai clic su Modifica . b. Nella sezione Azioni, associa l'avviso allo script di test.

5. Fare clic su **Salva**.

6. Nella pagina **Impostazione avviso**, seleziona l'avviso che hai aggiunto o modificato, quindi fai clic su **Test**.

Lo script viene eseguito con l'argomento "-test" e un avviso di notifica viene inviato agli indirizzi e-mail specificati al momento della creazione dell'avviso.

Gestire e monitorare i gruppi

È possibile creare gruppi in Unified Manager per gestire gli oggetti di archiviazione.

Comprendere i gruppi

È possibile creare gruppi in Unified Manager per gestire gli oggetti di archiviazione. Comprendere i concetti sui gruppi e il modo in cui le regole di gruppo consentono di aggiungere oggetti di archiviazione a un gruppo ti aiuterà a gestire gli oggetti di archiviazione nel tuo ambiente.

Che cosa è un gruppo

Un gruppo è una raccolta dinamica di oggetti di archiviazione eterogenei (cluster, SVM o volumi). È possibile creare gruppi in Unified Manager per gestire facilmente un set di oggetti di archiviazione. I membri di un gruppo potrebbero cambiare a seconda degli oggetti di archiviazione monitorati da Unified Manager in un dato momento.

- Ogni gruppo ha un nome univoco.
- È necessario configurare almeno una regola di gruppo per ogni gruppo.
- È possibile associare un gruppo a più di una regola di gruppo.
- Ogni gruppo può includere più tipi di oggetti di archiviazione, come cluster, SVM o volumi.
- Gli oggetti di archiviazione vengono aggiunti dinamicamente a un gruppo in base al momento in cui viene creata una regola di gruppo o al momento in cui Unified Manager completa un ciclo di monitoraggio.
- È possibile applicare contemporaneamente azioni a tutti gli oggetti di archiviazione in un gruppo, ad esempio impostando soglie per i volumi.

Come funzionano le regole di gruppo per i gruppi

Una regola di gruppo è un criterio definito per consentire l'inclusione di oggetti di archiviazione (volumi, cluster o SVM) in un gruppo specifico. È possibile utilizzare gruppi di condizioni o 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; a una regola di gruppo è associato un solo tipo di oggetto.
- Gli oggetti di archiviazione 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 ogni gruppo di condizioni può avere una o più condizioni.
- Gli oggetti di archiviazione possono appartenere a più gruppi in base alle regole di gruppo create.

Condizioni

È possibile creare più gruppi di condizioni e ogni 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 archiviazione sono inclusi nel gruppo.

Le condizioni all'interno di un gruppo di condizioni vengono eseguite utilizzando l'operatore logico AND. Devono essere soddisfatte tutte le condizioni di un gruppo di condizioni. Quando si crea o si modifica una regola di gruppo, viene creata una condizione che applica, seleziona e raggruppa solo gli oggetti di archiviazione che soddisfano tutte le condizioni nel gruppo di condizioni. È possibile utilizzare più condizioni all'interno di un gruppo di condizioni quando si desidera restringere l'ambito degli oggetti di archiviazione da includere in un gruppo.

È possibile creare condizioni con oggetti di archiviazione utilizzando i seguenti operandi e operatori e specificando il valore richiesto.

Tipo di oggetto di archiviazione	Operandi applicabili
Volume	• Nome dell'oggetto • Nome del cluster proprietario • Possedere il nome SVM • Annotazioni
SVM	• Nome dell'oggetto • Nome del cluster proprietario • Annotazioni
Grappolo	• Nome dell'oggetto • Annotazioni

Quando si seleziona l'annotazione come operando per un qualsiasi oggetto di archiviazione, è disponibile l'operatore "Is". Per tutti gli altri operandi, è possibile selezionare come operatore "Is" o "Contains".

- 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 dell'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 verificare la corrispondenza esatta del valore dell'operando con il valore fornito per l'operando selezionato.

Quando si seleziona l'operatore "Contiene", la condizione viene valutata in modo che soddisfi 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

Consideriamo un gruppo di condizioni per un volume con le due condizioni seguenti:

- 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 l'operatore logico OR e quindi applicati agli oggetti di archiviazione. Per essere inclusi in un gruppo, gli oggetti di archiviazione devono soddisfare uno dei gruppi di condizioni. Vengono combinati gli oggetti di archiviazione di tutti i gruppi di condizioni. È possibile utilizzare i gruppi di condizioni per ampliare l'ambito degli oggetti di archiviazione da includere in un gruppo.

Esempio di una regola di gruppo con gruppi di condizioni

Consideriamo due gruppi di condizioni per un volume, ciascuno contenente le due condizioni seguenti:

- 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 su SVM con il nome "data_svm".
- Gruppo di condizioni 2
 - Il nome contiene "vol"
 - Il valore di annotazione di data-priority è "critical". Il gruppo di condizioni 2 seleziona tutti i volumi che includono "vol" nei loro nomi e che sono annotati con il valore di annotazione data-priority come "critical".

Quando una regola di gruppo contenente questi due gruppi di condizioni viene applicata agli oggetti di archiviazione, i seguenti oggetti di archiviazione 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 data-priority “critical”.

Come funzionano le azioni di gruppo sugli oggetti di archiviazione

Un'azione di gruppo è un'operazione che viene eseguita su tutti gli oggetti di archiviazione in un gruppo. Ad esempio, è possibile configurare l'azione del gruppo di soglie del volume per modificare simultaneamente i valori delle soglie del volume di tutti i volumi in un gruppo.

I gruppi supportano tipi di azioni di gruppo univoci. È possibile avere 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 grado di un'azione di gruppo determina l'ordine in cui l'azione viene applicata agli oggetti di archiviazione. La pagina dei dettagli di un oggetto di archiviazione fornisce informazioni sull'azione di gruppo applicata all'oggetto di archiviazione.

Esempio di azioni di gruppo uniche

Si consideri un volume A appartenente ai gruppi G1 e G2 e per questi gruppi siano configurate le seguenti azioni di gruppo soglia di integrità del volume:

- `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 configurare le copie Snapshot del volume

IL `Change_capacity_threshold` l'azione di gruppo ha sempre la priorità sull' `Change_snapshot_copies` azione di gruppo e viene applicata al volume A. Quando Unified Manager completa un ciclo di monitoraggio, gli eventi correlati alla soglia di integrità del volume A vengono rivalutati in base al `Change_capacity_threshold` azione di gruppo. Non è possibile configurare un altro tipo di soglia del volume per l'azione di gruppo per il gruppo G1 o G2.

Aggiungi gruppi

È possibile creare gruppi per combinare cluster, volumi e macchine virtuali di archiviazione (SVM) per semplificare la gestione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile definire regole di gruppo per aggiungere o rimuovere membri dal gruppo e per modificare le azioni di gruppo per il gruppo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
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 gruppi

Puoi modificare il nome e la descrizione di un gruppo creato in Unified Manager.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Quando si modifica un gruppo per aggiornarne il nome, è necessario specificare un nome univoco; non è possibile utilizzare un nome di gruppo esistente.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Gruppi**, seleziona il gruppo che vuoi modificare, quindi fai clic su **Modifica**.
3. Nella finestra di dialogo **Modifica gruppo**, modifica il nome, la descrizione o entrambi per il gruppo.
4. Fare clic su **Salva**.

Elimina gruppi

È possibile eliminare un gruppo da Unified Manager quando non è più necessario.

Prima di iniziare

- Nessuno degli oggetti di archiviazione (cluster, SVM o volumi) deve essere associato a una regola di gruppo associata al gruppo che si desidera eliminare.
- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Gruppi**, seleziona il gruppo che desideri eliminare, quindi fai 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 saranno più mappate dopo l'eliminazione del gruppo.

Aggiungi regole di gruppo

È possibile creare regole di gruppo per un gruppo per aggiungere dinamicamente oggetti di archiviazione quali volumi, cluster o macchine virtuali di archiviazione (SVM) al gruppo. Per creare una regola di gruppo è necessario configurare almeno un gruppo di condizioni con almeno una condizione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Gli oggetti di archiviazione 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
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 **Tipo di oggetto di destinazione**, seleziona il tipo di oggetto di archiviazione che desideri raggruppare.

5. Nel campo **Gruppo**, seleziona il gruppo richiesto per il quale vuoi creare regole di gruppo.
6. Nella sezione **Condizioni**, eseguire i seguenti passaggi per creare una condizione, un gruppo di condizioni o entrambi:

Per creare....	Fai questo...
Una condizione	a. Selezionare un operando dall'elenco degli operandi. b. Selezionare Contiene o È come operatore. c. Inserisci un valore o selezionane uno dall'elenco disponibile.
Un gruppo di condizioni	a. Fare clic su Aggiungi gruppo di condizioni b. Selezionare un operando dall'elenco degli operandi. c. Selezionare Contiene o È come operatore. d. Inserisci un valore o selezionane uno dall'elenco disponibile. e. Fare clic su Aggiungi condizione per creare altre 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 i seguenti passaggi nella finestra di dialogo Aggiungi regola di gruppo:

Passi

1. Specificare un nome per la regola di gruppo.
2. Selezionare il tipo di oggetto come macchina virtuale di archiviazione (SVM).
3. Seleziona un gruppo dall'elenco dei gruppi.
4. Nella sezione Condizioni, seleziona **Nome oggetto** come operando.
5. Selezionare **Contiene** come operatore.
6. Inserisci il valore come `svm_data`.
7. Fare clic su **Aggiungi gruppo di condizioni**.
8. Selezionare **Nome oggetto** come operando.
9. Selezionare **Contiene** come operatore.
10. Inserisci il valore come `vol`.
11. Fare clic su **Aggiungi condizione**.
12. Ripetere i passaggi da 8 a 10 selezionando **data-priority** come operando nel passaggio 8, **Is** come operatore nel passaggio 9 e **critical** come valore nel passaggio 10.
13. Fare clic su **Aggiungi** per creare la condizione per la regola di gruppo.

Modifica le regole del 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 archiviazione da o verso un gruppo specifico.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Regole di gruppo**, seleziona la regola di gruppo che desideri modificare, quindi fai clic su **Modifica**.
3. Nella finestra di dialogo **Modifica regola di gruppo**, modificare il nome della regola di gruppo, il nome del gruppo associato, i gruppi di condizioni e le condizioni come richiesto.



Non è possibile modificare il tipo di oggetto di destinazione per una regola di gruppo.

4. Fare clic su **Salva**.

Elimina le regole del gruppo

È possibile eliminare una regola di gruppo da Active IQ Unified Manager quando non è più necessaria.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Quando una regola di gruppo viene eliminata, gli oggetti di archiviazione associati verranno rimossi dal gruppo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Regole di gruppo**, seleziona la regola di gruppo che desideri eliminare, quindi fai clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Aggiungi azioni di gruppo

È possibile configurare le azioni di gruppo che si desidera applicare agli oggetti di archiviazione in un gruppo. La configurazione delle azioni per un gruppo consente di risparmiare tempo, poiché non è necessario aggiungere queste azioni a ciascun oggetto singolarmente.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.

2. Nella scheda **Azioni di gruppo**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi azione di gruppo**, immettere un nome e una descrizione per l'azione.
4. Dal menu **Gruppo**, seleziona un gruppo per il quale desideri configurare l'azione.
5. Dal menu **Tipo di azione**, seleziona 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 azioni di gruppo

È possibile modificare i parametri dell'azione 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.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Azioni di gruppo**, seleziona l'azione di gruppo che desideri modificare, quindi fai clic su **Modifica**.
3. Nella finestra di dialogo **Modifica azione di 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 **Salva**.

Configurare le soglie di integrità del volume per i gruppi

È possibile configurare soglie di integrità del volume a livello di gruppo per capacità, copie snapshot, quote qtree, crescita e inode.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Il tipo di azione di gruppo soglia di integrità del volume viene applicato solo ai volumi di un gruppo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Azioni di gruppo**, fare clic su **Aggiungi**.
3. Inserisci un nome e una descrizione per l'azione di gruppo.
4. Dalla casella a discesa **Gruppo**, seleziona un gruppo per il quale desideri configurare l'azione di gruppo.
5. Selezionare **Tipo di azione** come soglia di integrità del volume.
6. Seleziona la categoria per la quale desideri impostare la soglia.
7. Immettere i valori richiesti per la soglia di integrità.

8. Fare clic su **Aggiungi**.

Elimina azioni di gruppo

È possibile eliminare un'azione di gruppo da Unified Manager quando non è più necessaria.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Quando si elimina l'azione di gruppo per la soglia di integrità del volume, le soglie globali vengono applicate agli oggetti di archiviazione in quel gruppo. Le soglie di integrità a livello di oggetto impostate sull'oggetto di archiviazione non sono interessate.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Azioni di gruppo**, seleziona l'azione di gruppo che desideri eliminare, quindi fai clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Riordina le azioni di gruppo

È possibile modificare l'ordine delle azioni di gruppo da applicare agli oggetti di archiviazione in un gruppo. Le azioni di gruppo vengono applicate agli oggetti di archiviazione in sequenza in base al loro grado. Il grado più basso viene assegnato all'azione di gruppo configurata per ultima. È possibile modificare il grado dell'azione di gruppo in base alle proprie esigenze.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile selezionare una singola riga o più righe e quindi eseguire più operazioni di trascinamento della selezione per modificare il grado delle azioni di gruppo. Tuttavia, è necessario salvare le modifiche affinché la ridefinizione delle priorità venga riflessa nella griglia delle azioni del gruppo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Gruppi**.
2. Nella scheda **Azioni di gruppo**, fare clic su **Riordina**.
3. Nella finestra di dialogo **Riordina azioni di gruppo**, trascinare e rilasciare le righe per riorganizzare la sequenza delle azioni di gruppo come desiderato.
4. Fare clic su **Salva**.

Assegnare la priorità agli eventi degli oggetti di archiviazione utilizzando le annotazioni

È possibile creare e applicare regole di annotazione agli oggetti di archiviazione in modo da poter identificare e filtrare tali oggetti in base al tipo di annotazione applicata e alla sua priorità.

Scopri di più sulle annotazioni

Comprendere i concetti sulle annotazioni aiuta a gestire gli eventi correlati agli oggetti di archiviazione nel proprio ambiente.

Cosa 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 di annotazione può essere associata dinamicamente agli oggetti di archiviazione utilizzando le regole di annotazione. Quando si associano oggetti di archiviazione ad annotazioni predefinite, è possibile filtrare e visualizzare gli eventi ad essi correlati. È possibile applicare annotazioni a cluster, volumi e macchine virtuali di archiviazione (SVM).

Ogni nome di annotazione può avere più valori; ogni coppia nome-valore può essere associata a un oggetto di archiviazione tramite 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 un evento su un volume v1 annotato con "data-center", l'e-mail generata indica la posizione del volume, "Boston", e questo consente di stabilire le priorità e risolvere il problema.

Come funzionano le regole di annotazione in Unified Manager

Una regola di annotazione è un criterio definito per annotare gli oggetti di archiviazione (volumi, cluster o macchine virtuali di archiviazione (SVM)). Per definire le regole di annotazione è possibile utilizzare sia gruppi di condizioni che condizioni.

- 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 solo un tipo di oggetto per una regola di annotazione.
- Unified Manager aggiunge o rimuove annotazioni dagli oggetti di archiviazione 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 ogni gruppo di condizioni può avere una o più condizioni.
- Gli oggetti di archiviazione 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 ogni 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 archiviazione.

Le condizioni all'interno di un gruppo di condizioni vengono eseguite utilizzando l'operatore logico AND. Devono essere soddisfatte tutte le condizioni di un gruppo di condizioni. Quando si crea o si modifica una regola di annotazione, viene creata una condizione che applica, seleziona e annota solo gli oggetti di archiviazione che soddisfano tutte le condizioni nel gruppo di condizioni. È possibile utilizzare più condizioni all'interno di un gruppo di condizioni quando si desidera restringere l'ambito degli oggetti di archiviazione da annotare.

È possibile creare condizioni con oggetti di archiviazione utilizzando i seguenti operandi e operatori e specificando il valore richiesto.

Tipo di oggetto di archiviazione	Operandi applicabili
Volume	• Nome dell'oggetto • Nome del cluster proprietario • Possedere il nome SVM • Annotazioni
SVM	• Nome dell'oggetto • Nome del cluster proprietario • Annotazioni
Grappolo	• Nome dell'oggetto • Annotazioni

Quando si seleziona l'annotazione come operando per un qualsiasi oggetto di archiviazione, è disponibile l'operatore "Is". Per tutti gli altri operandi, è possibile selezionare come operatore "Is" o "Contains". Quando si seleziona l'operatore "Is", la condizione viene valutata per verificare la corrispondenza esatta del valore dell'operando con il valore fornito per l'operando selezionato. Quando si seleziona l'operatore "Contiene", la condizione viene valutata in modo che soddisfi 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

Si consideri una regola di annotazione con un gruppo di condizioni per un volume con le due condizioni seguenti:

- Il nome contiene "vol"
- Il nome SVM è "data_svm"

Questa regola di annotazione annota tutti i volumi che includono "vol" nei loro nomi e che sono ospitati su 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 l'operatore logico OR e quindi applicati agli oggetti di archiviazione. Gli oggetti di archiviazione devono soddisfare i requisiti di uno dei gruppi di condizioni da annotare. Vengono annotati gli oggetti di archiviazione che soddisfano le condizioni di tutti i gruppi di condizioni. È possibile utilizzare gruppi di condizioni per ampliare l'ambito degli oggetti di archiviazione da annotare.

Esempio di una regola di annotazione con gruppi di condizioni

Si consideri una regola di annotazione con due gruppi di condizioni per un volume; ogni gruppo contiene le due condizioni seguenti:

- Gruppo di condizioni 1
 - Il nome contiene “vol”
 - Il nome SVM è “data_svm”. Questo gruppo di condizioni annota tutti i volumi che includono “vol” nei loro nomi e che sono ospitati su SVM con il nome “data_svm”.
- Gruppo di condizioni 2
 - Il nome contiene “vol”
 - Il valore di annotazione di data-priority è “critical”. Questo gruppo di condizioni annota tutti i volumi che includono “vol” nei loro nomi e che sono annotati con il valore di annotazione data-priority come “critical”.

Quando una regola di annotazione contenente questi due gruppi di condizioni viene applicata agli oggetti di archiviazione, vengono annotati i seguenti oggetti di archiviazione:

- 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 che ha i valori Mission critical, High e Low. Questi valori consentono di annotare gli oggetti di archiviazione in base alla priorità dei dati in essi contenuti. Non è possibile modificare o eliminare i valori di annotazione predefiniti.

- **Priorità dei dati: Missione critica**

Questa annotazione viene applicata agli oggetti di archiviazione che contengono dati critici per la missione. Ad esempio, gli oggetti che contengono applicazioni di produzione possono essere considerati mission critical.

- **Priorità dati: Alta**

Questa annotazione viene applicata agli oggetti di archiviazione che contengono dati ad alta priorità. Ad esempio, gli oggetti che ospitano applicazioni aziendali possono essere considerati ad alta priorità.

- **Priorità dati: Bassa**

Questa annotazione viene applicata agli oggetti di archiviazione che contengono dati a bassa priorità. Ad esempio, gli oggetti che si trovano su un archivio secondario, come destinazioni di backup e mirror, potrebbero avere una bassa priorità.

Aggiungi annotazioni in modo dinamico

Quando si creano annotazioni personalizzate, Unified Manager associa dinamicamente cluster, macchine virtuali di archiviazione (SVM) e volumi alle annotazioni utilizzando regole. Queste regole assegnano automaticamente le annotazioni agli oggetti di archiviazione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell’applicazione o Amministratore dell’archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
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 **Valori annotazione**, fare clic su **Aggiungi** per aggiungere valori all'annotazione.
5. Fare clic su **Salva**.

Aggiungi valori alle annotazioni

È possibile aggiungere valori alle annotazioni e quindi associare gli oggetti di archiviazione a una specifica coppia nome-valore dell'annotazione. L'aggiunta di valori alle annotazioni consente di gestire gli oggetti di archiviazione in modo più efficace.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Non è possibile aggiungere valori alle annotazioni predefinite.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella pagina **Annotazioni**, seleziona l'annotazione a cui vuoi aggiungere un valore, quindi fai 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**.

Elimina annotazioni

È possibile eliminare le annotazioni personalizzate e i relativi valori quando non sono più necessari.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- I valori di annotazione non devono essere utilizzati in altre annotazioni o regole di gruppo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella scheda **Annotazioni**, seleziona l'annotazione che desideri 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.

Visualizza l'elenco delle annotazioni e i dettagli

È possibile visualizzare l'elenco delle annotazioni associate dinamicamente a cluster, volumi e macchine virtuali di archiviazione (SVM). È inoltre possibile visualizzare dettagli quali la descrizione, l'autore, la data di creazione, i valori, le regole e gli oggetti associati all'annotazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella scheda **Annotazioni**, fare clic sul nome dell'annotazione per visualizzare i dettagli associati.

Elimina i valori dalle annotazioni

È possibile eliminare i valori associati alle annotazioni personalizzate quando tali valori non sono più applicabili all'annotazione.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Il valore di annotazione non deve essere associato ad alcuna regola di annotazione o regola di gruppo.

Non è possibile eliminare i valori dalle annotazioni predefinite.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nell'elenco delle annotazioni nella scheda **Annotazioni**, seleziona l'annotazione da cui desideri eliminare un valore.
3. Nell'area **Valori** della scheda **Annotazioni**, seleziona il valore che desideri eliminare, quindi fai clic su **Elimina**.
4. Nella finestra di dialogo **Avviso**, fare clic su **Sì**.

Il valore viene eliminato e non viene più visualizzato nell'elenco dei valori per l'annotazione selezionata.

Crea regole di annotazione

È possibile creare regole di annotazione che Unified Manager utilizza per annotare dinamicamente oggetti di archiviazione quali volumi, cluster o macchine virtuali di archiviazione (SVM).

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Gli oggetti di archiviazione 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella scheda **Regole di annotazione**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi regola di annotazione**, specificare un nome per la regola di

annotazione.

4. Nel campo **Tipo di oggetto di destinazione**, seleziona il tipo di oggetto di archiviazione che desideri annotare.
5. Nei campi **Applica annotazione**, seleziona l'annotazione e il valore dell'annotazione che desideri utilizzare.
6. Nella sezione Condizioni, eseguire l'azione appropriata per creare una condizione, un gruppo di condizioni o entrambi:

Per creare...	Fai questo...
Una condizione	a. Selezionare un operando dall'elenco degli operandi. b. Selezionare Contiene o È come operatore. c. Inserisci un valore o selezionane uno dall'elenco disponibile.
Un gruppo di condizioni	a. Fare clic su Aggiungi gruppo di condizioni. b. Selezionare un operando dall'elenco degli operandi. c. Selezionare Contiene o È come operatore. d. Inserisci un valore o selezionane uno dall'elenco disponibile. e. Fare clic su Aggiungi condizione per creare altre 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, eseguire i seguenti passaggi nella finestra di dialogo Aggiungi regola di annotazione, inclusa la configurazione di una condizione e l'aggiunta di un gruppo di condizioni:

Passi

1. Specificare un nome per la regola di annotazione.
2. Selezionare il tipo di oggetto di destinazione come macchina virtuale di archiviazione (SVM).
3. Selezionare un'annotazione dall'elenco delle annotazioni e specificare un valore.
4. Nella sezione Condizioni, seleziona **Nome oggetto** come operando.
5. Selezionare **Contiene** come operatore.
6. Inserisci il valore come `svm_data`.
7. Fare clic su **Aggiungi gruppo di condizioni**.
8. Selezionare **Nome oggetto** come operando.
9. Selezionare **Contiene** come operatore.
10. Inserisci il valore come `vol`.

11. Fare clic su **Aggiungi condizione**.
12. Ripetere i passaggi da 8 a 10 selezionando **data-priority** come operando nel passaggio 8, **Is** come operatore nel passaggio 9 e **mission-critical** come valore nel passaggio 10.
13. Fare clic su **Aggiungi**.

Aggiungere annotazioni manualmente ai singoli oggetti di archiviazione

È possibile annotare manualmente volumi, cluster e SVM selezionati senza utilizzare regole di annotazione. È possibile annotare un singolo oggetto di archiviazione o più oggetti di archiviazione e specificare la combinazione di coppie nome-valore richiesta per l'annotazione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Passare agli oggetti di archiviazione che si desidera annotare:

Per aggiungere annotazioni a...	Fai questo...
Cluster	a. Fare clic su Archiviazione > Cluster. b. Selezionare uno o più cluster.
Volumi	a. Fare clic su Archiviazione > Volumi. b. Seleziona uno o più volumi.
SVM	a. Fare clic su Archiviazione > SVM. b. Selezionare una o più SVM.

2. Fare clic su **Annota** e selezionare una coppia nome-valore.
3. Fare clic su **Applica**.

Modifica le 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 archiviazione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Le annotazioni vengono dissociate dagli oggetti di archiviazione quando si modificano le regole di annotazione associate.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella scheda **Regole di annotazione**, seleziona la regola di annotazione che desideri modificare, quindi

fai clic su **Azioni > Modifica**.

3. Nella finestra di dialogo **Modifica regola di annotazione**, modificare il nome della regola, il nome e il valore dell'annotazione, i gruppi di condizioni e le condizioni come richiesto.

Non è possibile modificare il tipo di oggetto di destinazione per una regola di annotazione.

4. Fare clic su **Salva**.

Configurare le 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 archiviazione. Gli oggetti di archiviazione che soddisfano la regola di annotazione vengono annotati con il valore specificato nella regola.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella scheda **Regole di annotazione**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi regola di annotazione**, immettere un nome per la regola.
4. Selezionare un tipo di oggetto dall'elenco Tipo di oggetto di destinazione, quindi selezionare un nome e un valore di annotazione dall'elenco.
5. Nella sezione **Condizioni** della finestra di dialogo, seleziona un operando e un operatore dall'elenco e immetti un valore di condizione oppure fai clic su **Aggiungi condizione** per creare una nuova condizione.
6. Fare clic su **Salva e aggiungi**.

Esempio di configurazione di una condizione per una regola di annotazione

Si consideri una condizione per il tipo di oggetto SVM, in cui il nome dell'oggetto contiene "svm_data".

Per configurare la condizione, eseguire i seguenti passaggi nella finestra di dialogo Aggiungi regola di annotazione:

Passi

1. Inserisci 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. Inserisci il valore come `svm_data`.
7. Fare clic su **Aggiungi**.

Elimina le regole di annotazione

È possibile eliminare le regole di annotazione da Active IQ Unified Manager quando non sono più necessarie.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Quando si elimina una regola di annotazione, l'annotazione viene dissociata e rimossa dagli oggetti di archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella scheda **Regole di annotazione**, seleziona la regola di annotazione che desideri eliminare, quindi fai clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, fare clic su **Sì** per confermare l'eliminazione.

Riordina le regole di annotazione

È possibile modificare l'ordine in cui Unified Manager applica le regole di annotazione agli oggetti di archiviazione. Le regole di annotazione vengono applicate agli oggetti di archiviazione in sequenza in base al loro rango. Quando si configura una regola di annotazione, il grado è minimo. Ma puoi modificare il grado della regola di annotazione in base alle tue esigenze.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile selezionare una singola riga o più righe ed eseguire numerose operazioni di trascinamento della selezione per modificare il grado delle regole di annotazione. Tuttavia, è necessario salvare le modifiche affinché la ridefinizione delle priorità venga visualizzata nella scheda Regole di annotazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Annotazioni**.
2. Nella scheda **Regole di annotazione**, fare clic su **Riordina**.
3. Nella finestra di dialogo **Riordina regola annotazione**, trascinare e rilasciare una o più righe per riorganizzare la sequenza delle regole di annotazione.
4. Fare clic su **Salva**.

Per visualizzare il riordino è necessario salvare le modifiche.

Invia un pacchetto di supporto tramite l'interfaccia utente Web e la console di manutenzione

Dovresti inviare un pacchetto di supporto quando il problema che hai riscontrato richiede una diagnosi e una risoluzione dei problemi più dettagliate di quelle fornite da un messaggio AutoSupport. È possibile inviare un pacchetto di supporto al supporto tecnico tramite l'interfaccia utente Web di Unified Manager e la console di manutenzione.

Unified Manager memorizza al massimo due pacchetti di supporto completo e tre pacchetti di supporto leggero contemporaneamente.

Informazioni correlate

Invia messaggi AutoSupport e pacchetti di supporto al supporto tecnico

La pagina AutoSupport consente di inviare messaggi AutoSupport predefiniti e su richiesta al team di supporto tecnico per garantire il corretto funzionamento del tuo ambiente e per aiutarti a mantenerne l'integrità. AutoSupport è abilitato per impostazione predefinita e non deve essere disabilitato per poter usufruire dei vantaggi di NetAppActive IQ.

È possibile inviare informazioni diagnostiche sul sistema e dati dettagliati sul server Unified Manager in un messaggio quando e se necessario, pianificare l'invio periodico di un messaggio o persino generare e inviare pacchetti di supporto al team di supporto tecnico.



Un utente con ruolo di amministratore di storage può generare e inviare messaggi AutoSupport su richiesta e pacchetti di supporto al supporto tecnico. Tuttavia, solo un amministratore o un utente addetto alla manutenzione può abilitare o disabilitare AutoSupport periodico e configurare le impostazioni HTTP come descritto nella sezione Impostazione del server proxy HTTP. In un ambiente che necessita di utilizzare un server proxy HTTP, la configurazione deve essere completata prima che un amministratore di storage possa inviare messaggi AutoSupport su richiesta e pacchetti di supporto al supporto tecnico.

Invia messaggi AutoSupport su richiesta

È possibile generare e inviare un messaggio su richiesta al supporto tecnico, a un destinatario e-mail specificato o a entrambi.

Passi

1. Vai su **Generale** > * AutoSupport* ed esegui una o entrambe le seguenti azioni:
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 e-mail specifico, selezionare la casella di controllo **Invia al destinatario e-mail** e immettere l'indirizzo e-mail del destinatario.
4. Fare clic su **Salva**.
5. Fare clic su **Genera e invia AutoSupport**.

Abilita AutoSupport periodico

È possibile inviare periodicamente messaggi specifici e predefiniti al supporto tecnico per la diagnosi e la risoluzione dei problemi. Questa funzionalità è abilitata per impostazione predefinita. Se disabilitata, un amministratore o un utente addetto alla manutenzione può abilitare le impostazioni.

Passi

1. Vai su **Generale** > * AutoSupport*.
2. Nella sezione AutoSupport periodico, seleziona la casella di controllo **Abilita l'invio periodico dei dati AutoSupport ad Active IQ**.
3. Se necessario, definire il nome, la porta e le informazioni di autenticazione per il server proxy HTTP come descritto nella sezione Configurazione del server proxy HTTP.
4. Fare clic su **Salva**.

Carica il pacchetto di supporto su richiesta

È possibile generare e inviare un pacchetto di supporto al supporto tecnico in base alle esigenze di risoluzione dei problemi. Unified Manager memorizza solo i due bundle di supporto generati più di recente. I vecchi pacchetti di supporto 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 essere completati, 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 pacchetto di supporto leggero che contiene solo 30 giorni di log e record del database di configurazione, escludendo i dati sulle prestazioni, i file di registrazione delle acquisizioni e il dump dell'heap del server.

Passi

1. Vai su **Generale** > * AutoSupport*.
2. Nella sezione Pacchetto di supporto su richiesta, fare clic su **Genera e invia pacchetto di supporto**.
3. Per inviare un pacchetto di supporto leggero al supporto tecnico, nel pop-up Genera e invia pacchetto di supporto, seleziona la casella di controllo **Genera pacchetto di supporto leggero**.
4. In alternativa, per inviare un pacchetto di supporto completo, seleziona la casella di controllo **Genera pacchetto di supporto completo**. Selezionare i tipi di dati specifici da includere o escludere nel pacchetto di supporto.



Anche se non si seleziona alcun tipo di dati, il pacchetto 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 archiviato localmente nel server Unified Manager. Il pacchetto di supporto generato è disponibile per un utilizzo successivo nella directory /support sui sistemi VMware, in /opt/netapp/data/support/ sui sistemi Linux e in ProgramData\NetApp\OnCommandAppData\ocum\support sui sistemi Windows.
6. Fare clic su **Invia**.

Imposta il server proxy HTTP

È possibile designare un proxy per fornire l'accesso a Internet per inviare contenuti AutoSupport al supporto se l'ambiente non fornisce un accesso diretto dal server Unified Manager. Questa sezione è disponibile solo per gli utenti amministratori e manutentori.

• Utilizza proxy HTTP

Seleziona 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.

• Utilizza l'autenticazione

Seleziona questa casella se devi 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.

Accedi 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.

Prima di iniziare

È necessario aver installato e configurato Unified Manager.

Dopo 15 minuti di inattività, la console di manutenzione effettua la disconnessione.



Se installato su VMware, se hai già effettuato l'accesso come utente di manutenzione tramite la console VMware, non puoi effettuare l'accesso contemporaneamente tramite Secure Shell.

Fare un passo

1. Per accedere alla console di manutenzione, seguire questi passaggi:

Su questo sistema operativo...	Segui questi passaggi...
VMware	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo dell'appliance virtuale Unified Manager. b. Accedi alla console di manutenzione utilizzando il tuo nome utente e la tua password di manutenzione.
Linux	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager. b. Accedi al sistema con il nome utente di manutenzione (umadmin) e la password. c. Inserisci il comando <code>maintenance_console</code> e premere Invio.
Finestre	a. Accedi al sistema Unified Manager con le credenziali di amministratore. b. Avvia PowerShell come amministratore di Windows. c. Inserisci il comando <code>maintenance_console</code> e premere Invio.

Viene visualizzato il menu della console di manutenzione di Unified Manager.

Genera e carica un pacchetto di supporto

È possibile generare un pacchetto di supporto contenente informazioni diagnostiche, in modo da poterlo inviare al supporto tecnico per ottenere assistenza nella 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 su NetApp dalla console di manutenzione.

Prima di iniziare

È necessario avere accesso alla console di manutenzione come utente addetto alla manutenzione.

Poiché alcuni tipi di dati di supporto possono utilizzare una grande quantità di risorse del cluster o richiedere molto tempo per essere completati, 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 pacchetto di supporto leggero che contiene solo 30 giorni di log e record del database di configurazione, escludendo i dati sulle prestazioni, i file di registrazione delle acquisizioni e il dump dell'heap del server.

Unified Manager memorizza solo i due bundle di supporto generati più di recente. I vecchi pacchetti di supporto vengono eliminati dal sistema.

Passi

1. Nel **Menu principale** della console di manutenzione, selezionare **Supporto/Diagnostica**.
2. Selezionare **Genera pacchetto di supporto leggero** o **Genera pacchetto di supporto** a seconda del livello di dettaglio che si desidera avere nel pacchetto di supporto.
3. Se si sceglie il pacchetto di supporto completo, selezionare o deselezionare i seguenti tipi di dati da includere o escludere nel pacchetto di supporto:

- **svuotamento del database**

Un dump del database MySQL Server.

- **cumulo di rifiuti**

Un'istantanea dello stato dei principali processi del server Unified Manager. Questa opzione è disabilitata per impostazione predefinita e dovrebbe essere selezionata solo quando richiesto dall'assistenza clienti.

- **registrazioni di acquisizione**

Una registrazione di tutte le comunicazioni tra Unified Manager e i cluster monitorati.



Se deselezioni tutti i tipi di dati, il pacchetto di supporto verrà comunque generato con altri dati di Unified Manager.

4. Tipo **g** , quindi premere Invio per generare il pacchetto di supporto.

Poiché la generazione di un bundle di supporto è un'operazione che richiede molta memoria, ti verrà chiesto di verificare se sei sicuro di voler generare il bundle di supporto in questo momento.

5. Tipo **y** , quindi premere Invio per generare il pacchetto di supporto.

Se non si desidera generare il pacchetto di supporto in questo momento, digitare **n** e quindi premere Invio.

6. Se hai incluso i file di dump del database nel pacchetto di supporto completo, ti verrà chiesto di specificare il periodo di tempo per il quale desideri includere le statistiche sulle prestazioni. L'inclusione delle statistiche sulle prestazioni può richiedere molto tempo e spazio, quindi è possibile anche eseguire il dump del database senza includere le statistiche sulle prestazioni:

- a. Inserire la data di inizio nel formato AAAAMMGG.

Ad esempio, inserisci 20210101 per il 1° gennaio 2021. Entra *n* se non si desidera che vengano incluse le statistiche sulle prestazioni.

- b. Inserire il numero di giorni di statistiche da includere, a partire dalle ore 00:00 della data di inizio specificata.

È possibile immettere un numero compreso tra 1 e 10.

Se si includono statistiche sulle prestazioni, il sistema visualizza il periodo di tempo per il quale verranno raccolte tali statistiche.

7. Dopo aver creato il pacchetto di supporto, ti verrà chiesto se desideri caricarlo su NetApp. Tipo *y* e quindi premere Invio.

Ti verrà chiesto di inserire il numero del tuo caso di supporto.

8. Se si dispone già di un numero di pratica, inserirlo e premere Invio. Altrimenti basta premere Invio.

Il pacchetto di supporto viene caricato su NetApp.

Se il server Unified Manager non è connesso a Internet o se per qualsiasi altro motivo non riesci a caricare il pacchetto di supporto, puoi recuperarlo e inviarlo manualmente. È possibile recuperarlo utilizzando un client SFTP oppure i comandi CLI di UNIX o Linux. Nelle installazioni Windows è possibile utilizzare Desktop remoto (RDP) per recuperare il pacchetto di supporto.

Il pacchetto 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 capacità degli utenti di Unified Manager"](#)

Recupera il pacchetto di supporto utilizzando un client Windows

Se sei un utente Windows, puoi scaricare e installare uno strumento per recuperare il pacchetto di supporto dal tuo 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 puoi utilizzare.

Prima di iniziare

Per eseguire questa attività è necessario essere un utente addetto alla manutenzione.

È necessario utilizzare uno strumento che supporti SCP o SFTP.

Passi

1. Scarica e installa uno strumento per recuperare il pacchetto di supporto.
2. Aprire lo strumento.
3. Connettiti al tuo server di gestione Unified Manager tramite SFTP.

Lo strumento visualizza il contenuto della directory /support e consente di visualizzare tutti i pacchetti di supporto esistenti.

4. Selezionare la directory di destinazione per il pacchetto di supporto che si desidera copiare.
5. Seleziona il pacchetto di supporto che desideri copiare e utilizza lo strumento per copiare il file dal server Unified Manager al tuo sistema locale.

Recupera il pacchetto di supporto utilizzando un client UNIX o Linux

Se sei un utente UNIX o Linux, puoi recuperare il bundle di supporto dalla tua vApp utilizzando l'interfaccia della riga di comando (CLI) sul tuo server client Linux. Per recuperare il pacchetto di supporto è possibile utilizzare SCP o SFTP.

Prima di iniziare

Per eseguire questa attività è necessario essere un utente addetto alla manutenzione.

È necessario aver generato un bundle di supporto utilizzando la console di manutenzione e avere a disposizione il nome del bundle di supporto.

Passi

1. Accedi alla CLI tramite Telnet o la console, utilizzando il tuo server client Linux.
2. Accedi al/support elenco.
3. Recupera il pacchetto di supporto e copialo nella directory locale utilizzando il seguente comando:

Se stai utilizzando...	Quindi utilizzare il seguente comando...
SCP	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
SFTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

Il nome del pacchetto di supporto ti viene fornito quando lo generi tramite la console di manutenzione.

4. Inserire la password dell'utente addetto alla manutenzione.

Esempi

L'esempio seguente utilizza 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
```

L'esempio seguente utilizza SFTP per recuperare il pacchetto 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
```

Invia un pacchetto di supporto al supporto tecnico

Quando un problema richiede informazioni di diagnosi e risoluzione dei problemi più dettagliate di quelle fornite da un messaggio AutoSupport , è possibile inviare un pacchetto di supporto al supporto tecnico.

Prima di iniziare

Per poter inviare il pacchetto di supporto al supporto tecnico, è necessario avere accesso.

È necessario disporre di un numero di pratica generato tramite il sito web del supporto tecnico.

Passi

1. Accedi al sito di supporto NetApp .
2. Carica 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 flusso di lavoro sono comuni a molti flussi di lavoro in 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 i dettagli su volumi, macchine virtuali di archiviazione (SVM), aggregati e così via.

Componenti del cluster e perché possono essere in competizione

È possibile identificare i problemi di prestazioni del cluster quando un componente del cluster entra in conflitto. Le prestazioni dei carichi di lavoro che utilizzano il componente rallentano e il tempo di risposta (latenza) alle richieste dei client aumenta, il che attiva un evento in Unified Manager.

Un componente in competizione non può funzionare a un livello ottimale. Le sue prestazioni sono diminuite e le prestazioni di altri componenti del cluster e carichi di lavoro, denominati *vittime*, potrebbero aver aumentato la latenza. Per mettere un componente fuori gioco, è necessario ridurre il suo carico di lavoro o aumentare la sua capacità di gestire più lavoro, in modo che le prestazioni possano tornare a livelli normali. Poiché Unified Manager raccoglie e analizza le prestazioni del carico di lavoro a intervalli di cinque minuti, rileva solo quando un componente del cluster viene costantemente sovrautilizzato. Non vengono rilevati picchi transitori di sovrautilizzo che durano solo per un breve periodo nell'intervallo di cinque minuti.

Ad esempio, un aggregato di archiviazione potrebbe essere in competizione perché uno o più carichi di lavoro su di esso competono per soddisfare le loro richieste di I/O. Altri carichi di lavoro sull'aggregato potrebbero essere interessati, con conseguente riduzione delle prestazioni. Per ridurre la quantità di attività sull'aggregato, è possibile adottare diverse misure, ad esempio spostando uno o più carichi di lavoro su un aggregato o un nodo meno occupato, per diminuire la richiesta complessiva di carico di lavoro sull'aggregato corrente. Per un gruppo di policy QoS, è possibile modificare il limite di throughput o spostare i carichi di lavoro in un gruppo di policy diverso, in modo che non vengano più limitati.

Unified Manager monitora i seguenti componenti del cluster per avvisarti quando sono 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 ad attendere il completamento delle transazioni "transfer ready" prima che il cluster possa rispondere a una richiesta di I/O. Se il componente di rete è in competizione, significa che l'elevato tempo di attesa a livello di protocollo sta influenzando la latenza di uno o più carichi di lavoro.

- **Elaborazione di rete**

Rappresenta il componente software nel cluster coinvolto nell'elaborazione I/O tra il livello del protocollo e il cluster. L'elaborazione della rete di gestione del nodo potrebbe essere cambiata da quando è stato rilevato l'evento. Se il componente di elaborazione della rete è in competizione, significa che l'elevato utilizzo del nodo di elaborazione della rete sta influenzando la latenza di uno o più carichi di lavoro.

Quando si utilizza un cluster All SAN Array in una configurazione attiva-attiva, il valore di latenza dell'elaborazione di rete viene visualizzato per entrambi i nodi, in modo da poter verificare che i nodi condividano equamente il carico.

- **Limite QoS massimo**

Rappresenta l'impostazione massima (picco) della velocità effettiva del gruppo di policy QoS (Quality of Service) di archiviazione 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 limitati dal limite di throughput impostato, il che influisce sulla latenza di uno o più di tali carichi di lavoro.

- **Limite QoS minimo**

Rappresenta la latenza di un carico di lavoro causata dall'impostazione minima (prevista) della velocità effettiva QoS assegnata ad altri carichi di lavoro. Se il valore minimo di QoS impostato su determinati carichi di lavoro utilizza la maggior parte della larghezza di banda per garantire la produttività promessa, altri carichi di lavoro saranno limitati e vedranno una maggiore latenza.

- **Interconnessione cluster**

Rappresenta i cavi e gli adattatori con cui i nodi del cluster sono fisicamente collegati. Se il componente di interconnessione del cluster è in conflitto, significa che l'elevato tempo di attesa per le richieste di I/O nell'interconnessione del cluster sta influenzando la latenza di uno o più carichi di lavoro.

- *** Data Processing***

Rappresenta il componente software nel cluster coinvolto nell'elaborazione I/O tra il cluster e l'aggregato di archiviazione 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 dati è in conflitto, significa che l'elevato utilizzo del nodo di elaborazione dati sta influenzando la latenza di uno o più carichi di lavoro.

- **Attivazione del volume**

Rappresenta il processo che tiene traccia dell'utilizzo di tutti i volumi attivi. Negli ambienti di grandi dimensioni in cui sono attivi più di 1000 volumi, questo processo tiene traccia di quanti volumi critici devono accedere alle risorse tramite il nodo contemporaneamente. Quando il numero di volumi attivi contemporaneamente supera la soglia massima consigliata, alcuni volumi non critici subiranno latenza come indicato qui.

- * Risorse MetroCluster *

Rappresenta le risorse MetroCluster , tra cui NVRAM e collegamenti interswitch (ISL), utilizzati per eseguire il mirroring dei dati tra cluster in una configurazione MetroCluster . Se il componente MetroCluster è in conflitto, significa che l'elevata velocità di scrittura dei carichi di lavoro sul cluster locale oppure un problema di integrità del collegamento sta influenzando la latenza di uno o più carichi di lavoro sul cluster locale. Se il cluster non è in una configurazione MetroCluster , questa icona non viene visualizzata.

- **Operazioni aggregate o SSD aggregate**

Rappresenta l'aggregato di archiviazione su cui vengono eseguiti i carichi di lavoro. Se il componente aggregato è in competizione, significa che l'elevato utilizzo dell'aggregato sta influenzando la latenza di uno o più carichi di lavoro. Un aggregato è costituito da tutti gli HDD, oppure da un mix di HDD e SSD (un aggregato Flash Pool) oppure da un mix di HDD e un livello cloud (un aggregato FabricPool). Un "aggregato SSD" è costituito da tutti gli SSD (un aggregato all-flash) o da un mix di SSD e un livello cloud (un aggregato FabricPool).

- **Latenza del cloud**

Rappresenta il componente software nel cluster coinvolto nell'elaborazione I/O tra il cluster e il livello cloud su cui sono archiviati i dati utente. Se il componente di latenza del cloud è in conflitto, significa che una grande quantità di letture da volumi ospitati sul livello cloud sta influenzando la latenza di uno o più carichi di lavoro.

- **Sincronizza SnapMirror**

Rappresenta il componente software nel cluster coinvolto nella replica dei dati utente dal volume primario al volume secondario in una relazione sincrona SnapMirror . Se il componente di sincronizzazione SnapMirror è in conflitto, significa che l'attività delle operazioni sincrone SnapMirror sta influenzando la latenza di uno o più carichi di lavoro.

Pagina dei dettagli del volume/salute

È possibile utilizzare la pagina Dettagli volume/integrità per visualizzare informazioni dettagliate su un volume selezionato, ad esempio capacità, efficienza di archiviazione, configurazione, protezione, annotazione ed eventi generati. È inoltre possibile visualizzare informazioni sugli oggetti correlati e sugli avvisi correlati per quel volume.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per il volume selezionato:

- **Passa alla visualizzazione delle prestazioni**

Consente di accedere alla pagina dei dettagli Volume/Prestazioni.

- **Azioni**

- Aggiungi avviso

Consente di aggiungere un avviso al volume selezionato.

- Modifica 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 sulla relazione di protezione:

- Modificare

Avvia la finestra di dialogo Modifica relazione, che consente di modificare i criteri, le pianificazioni e le velocità di trasferimento massime SnapMirror esistenti per una relazione di protezione esistente.

- Aborto

Interrompe i trasferimenti in corso per una relazione selezionata. Facoltativamente, consente di rimuovere il checkpoint di riavvio per i trasferimenti diversi dal trasferimento di base. Non è possibile rimuovere il checkpoint per un trasferimento di base.

- Quiesce

Disattiva temporaneamente gli aggiornamenti pianificati per una relazione selezionata. I trasferimenti già in corso devono essere completati prima che la relazione venga sospesa.

- Rottura

Interrompe la relazione tra i volumi di origine e di destinazione e modifica la destinazione in un volume di lettura-scrittura.

- Rimuovere

Elimina definitivamente 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.

- Riprendere

Abilita i trasferimenti pianificati per una relazione inattiva. Al successivo intervallo di trasferimento pianificato, viene utilizzato un checkpoint di riavvio, se presente.

- **Risincronizzare**

Consente di risincronizzare una relazione precedentemente interrotta.

- **Inizializza/Aggiorna**

Consente di eseguire un primo trasferimento della baseline su una nuova relazione di protezione oppure 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, rendendo l'origine una copia della destinazione originale. Il contenuto dell'origine viene sovrascritto dal contenuto della destinazione e tutti i dati più recenti rispetto ai dati presenti nella copia Snapshot comune vengono eliminati.

- **Ripristinare**

Consente di ripristinare i dati da un volume a un altro. Per informazioni, vedere ["Ripristino dei dati tramite la pagina Dettagli volume/integrità"](#).



Il pulsante Ripristina e i pulsanti Operazione relazione non sono disponibili per i volumi che si trovano in relazioni di protezione sincrona.

- **Visualizza volumi**

Consente di passare alla vista Salute: Tutti i volumi.

Scheda Capacità

La scheda Capacità visualizza i dettagli sul volume selezionato, come la sua capacità fisica, la capacità logica, le impostazioni della soglia, la capacità della quota e informazioni su qualsiasi operazione di spostamento del volume:

- **Capacità fisica**

Descrive in dettaglio la capacità fisica del volume:

- **Overflow dell'istantanea**

Visualizza lo spazio dati utilizzato dalle copie Snapshot.

- **Usato**

Visualizza lo spazio utilizzato dai dati nel volume.

- **Avvertimento**

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 è stato generato l'evento Spazio a rischio nel volume con provisioning sottile e che lo spazio nel volume con provisioning sottile è a rischio a causa di problemi di capacità aggregata. La capacità inutilizzabile viene visualizzata solo per i volumi con provisioning ridotto.

- Grafico dei dati

Visualizza la capacità dati totale e la capacità dati utilizzata del volume.

Se l'aumento automatico è abilitato, il grafico dei dati visualizza anche lo spazio disponibile nell'aggregato. Il grafico dei dati mostra lo spazio di archiviazione effettivo che può essere utilizzato dai dati nel volume, che può essere uno dei seguenti:

- Capacità dati effettiva del volume per le seguenti condizioni:
 - L'aumento automatico è disabilitato.
 - Il volume abilitato per l'aumento automatico ha raggiunto la dimensione massima.
 - Il volume con provisioning spesso abilitato per l'aumento automatico non può crescere ulteriormente.
- Capacità dati del volume dopo aver considerato la dimensione massima del volume (per volumi con provisioning sottile e per volumi con provisioning spesso quando l'aggregato ha spazio sufficiente affinché il volume raggiunga la dimensione massima)
- Capacità dati del volume dopo aver considerato la successiva possibile dimensione di aumento automatico (per volumi con provisioning spesso che hanno una soglia percentuale di aumento automatico)

- Grafico delle copie snapshot

Questo grafico viene visualizzato solo quando la capacità Snapshot utilizzata o la riserva Snapshot non è zero.

Entrambi i grafici mostrano la capacità per cui la capacità Snapshot supera la riserva Snapshot se la capacità Snapshot utilizzata supera la riserva Snapshot.

- **Capacità logica**

Visualizza le caratteristiche dello spazio logico del volume. Lo spazio logico indica la dimensione reale dei dati memorizzati sul disco, senza applicare i risparmi derivanti dall'utilizzo delle tecnologie di efficienza di archiviazione ONTAP .

- Segnalazione dello spazio logico

Visualizza se il volume ha configurato la segnalazione dello spazio logico. Il valore può essere Abilitato, Disabilitato o Non applicabile. Per i volumi su versioni precedenti di ONTAP o su volumi che non supportano la segnalazione dello spazio logico viene visualizzato "Non applicabile".

- Usato

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'applicazione dello spazio logico è configurata per i volumi con provisioning sottile. Se

impostato su Abilitato, la dimensione logica utilizzata del volume non può essere maggiore della dimensione del volume fisico attualmente impostata.

- **Autocrescita**

Indica se il volume aumenta automaticamente quando lo spazio è esaurito.

- **Garanzia di spazio**

Visualizza il controllo delle impostazioni FlexVol volume quando un volume rimuove blocchi liberi da un aggregato. È quindi garantito che questi blocchi siano disponibili per la scrittura sui file nel volume. La garanzia dello spazio può essere impostata su uno dei seguenti:

- Nessuno

Non è configurata alcuna garanzia di spazio per il volume.

- File

È garantita la dimensione completa dei file scritti in modo sparso (ad esempio, LUN).

- Volume

È garantita la dimensione completa del volume.

- Parziale

Il volume FlexCache riserva spazio in base alle sue dimensioni. Se la dimensione del volume FlexCache è pari o superiore a 100 MB, per impostazione predefinita lo spazio minimo garantito è impostato su 100 MB. Se la dimensione del volume FlexCache è inferiore a 100 MB, la garanzia di spazio minimo è impostata sulla dimensione del volume FlexCache. Se in un secondo momento le dimensioni del volume FlexCache aumentano, la garanzia di spazio minimo non verrà 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 dati**

Visualizza la quantità di spazio fisico utilizzata 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 viene generato l'evento Spazio a rischio del volume con thin provisioning per i volumi con thin provisioning, vengono visualizzate la quantità di spazio utilizzata dal volume (capacità utilizzata) e la quantità di spazio disponibile nel volume ma che non può essere utilizzata (capacità inutilizzabile) a causa di problemi di capacità aggregata.

- **Riserva istantanea**

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 totale di snapshot.

Quando viene generato l'evento Spazio a rischio del volume con thin provisioning per i volumi con thin provisioning, vengono visualizzate la quantità di spazio utilizzata dalle copie snapshot (capacità utilizzata) e la quantità di spazio disponibile nel volume ma che non può essere utilizzata per creare copie snapshot (capacità inutilizzabile) a causa di problemi di capacità aggregata.

- **Soglie di volume**

Visualizza le seguenti soglie di capacità del volume:

- Soglia quasi piena

Specifica la percentuale in cui un volume è quasi pieno.

- Soglia completa

Specifica la percentuale di riempimento di un volume.

- **Altri dettagli**

- Crescita automatica dimensione massima

Visualizza la dimensione massima fino alla quale il volume può aumentare automaticamente. Il valore predefinito è il 120% della dimensione del volume al momento della creazione. Questo campo viene visualizzato solo quando l'aumento automatico è abilitato per il volume.

- Capacità impegnata della quota Qtree

Visualizza lo spazio riservato nelle quote.

- Capacità impegnata in eccesso per quota Qtree

Visualizza la quantità di spazio che può essere utilizzata prima che il sistema generi l'evento Volume Qtree Quota Overcommitted.

- Riserva frazionaria

Controlla la dimensione della riserva di sovrascrittura. Per impostazione predefinita, la riserva frazionaria è impostata su 100, a indicare che il 100 percento dello spazio riservato richiesto è riservato, in modo che gli oggetti siano completamente protetti dalle sovrascritture. Se la riserva frazionaria è inferiore al 100 percento, lo spazio riservato per tutti i file con spazio riservato in quel volume viene ridotto alla percentuale di riserva frazionaria.

- Istantanea del tasso di crescita giornaliero

Visualizza la modifica (in percentuale o in KB, MB, GB e così via) che si verifica ogni 24 ore nelle copie Snapshot nel volume selezionato.

- Giorni mancanti alla fine dell'istantanea

Visualizza il numero stimato di giorni rimanenti prima che lo spazio riservato alle copie Snapshot nel volume raggiunga la soglia specificata.

Il campo Giorni di snapshot al completamento visualizza un valore Non applicabile quando il tasso di crescita delle copie snapshot nel volume è zero o negativo, oppure quando non ci sono dati sufficienti per calcolare il tasso di crescita.

- Eliminazione automatica snapshot

Specifica se le copie Snapshot vengono eliminate automaticamente per liberare spazio quando una scrittura su un volume non riesce a causa della mancanza di spazio nell'aggregato.

- Copie istantanee

Visualizza informazioni sulle copie Snapshot nel volume.

Il numero di copie Snapshot nel volume viene visualizzato come collegamento. Facendo clic sul collegamento si apre la finestra di dialogo 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 nel momento in cui si fa clic sull'icona. Ciò potrebbe comportare una differenza tra il conteggio delle copie Snapshot visualizzato nella topologia e il numero di copie Snapshot elencate quando si fa clic sull'icona.

- **Spostamento del volume**

Visualizza lo stato dell'operazione di spostamento del volume corrente o dell'ultima operazione 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 l'ora di fine stimata.

Visualizza anche il numero di operazioni di spostamento del volume eseguite sul volume selezionato. È possibile visualizzare ulteriori informazioni sulle operazioni di spostamento del volume facendo clic sul collegamento **Cronologia spostamenti volume**.

Scheda di configurazione

La scheda Configurazione visualizza i dettagli sul volume selezionato, come la politica di esportazione, il tipo di RAID, la capacità e le caratteristiche relative all'efficienza di archiviazione del volume:

- **Panoramica**

- Nome e cognome

Visualizza il nome completo del volume.

- Aggregati

Visualizza il nome dell'aggregato su cui risiede il volume oppure il numero di aggregati su cui risiede il volume FlexGroup .

- Politica di suddivisione in livelli

Visualizza la policy di suddivisione in livelli impostata per il volume; se il volume è distribuito su un aggregato abilitato per FabricPool. Il criterio può essere Nessuno, Solo snapshot, Backup, Automatico o Tutto.

- VM di archiviazione

Visualizza il nome dell'SVM che contiene il volume.

- Percorso di giunzione

Visualizza lo stato del percorso, che può essere attivo o inattivo. Viene visualizzato anche il percorso nell'SVM su cui è montato il volume. È possibile fare clic sul collegamento **Cronologia** per visualizzare le cinque modifiche più recenti apportate al percorso dell'incrocio.

- Politica di esportazione

Visualizza il nome del criterio di esportazione creato per il volume. È possibile fare clic sul collegamento per visualizzare i dettagli sui criteri di esportazione, sui protocolli di autenticazione e sull'accesso abilitato sui volumi appartenenti all'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 Lettura-scrittura, Condivisione del carico, Protezione dati, Cache dati o Temporaneo.

- Tipo RAID

Visualizza il tipo RAID del volume selezionato. Il tipo RAID può essere RAID0, RAID4, RAID-DP o RAID-TEC.



Per i volumi FlexGroup potrebbero essere visualizzati più tipi di RAID perché i volumi costituenti dei FlexGroup possono essere aggregati di tipi diversi.

- Tipo SnapLock

Visualizza il tipo di SnapLock dell'aggregato che contiene il volume.

- Scadenza SnapLock

Visualizza la data di scadenza del volume SnapLock .

- **Capacità**

- Provisioning sottile

Visualizza se il thin provisioning è configurato per il volume.

- Crescita automatica

Visualizza se il volume flessibile aumenta automaticamente all'interno di un aggregato.

- Eliminazione automatica snapshot

Specifica se le copie Snapshot vengono eliminate automaticamente per liberare spazio quando una scrittura su un volume non riesce a causa della mancanza di spazio nell'aggregato.

- Quote

Specifica se le quote sono abilitate per il volume.

- **Efficienza**

- Compressione

Specifica se la compressione è abilitata o disabilitata.

- Deduplicazione

Specifica se la deduplicazione è abilitata o disabilitata.

- Modalità di deduplicazione

Specifica se l'operazione di deduplicazione abilitata su un volume è un'operazione manuale, pianificata o basata su criteri. Se la modalità è impostata su Pianificato, viene visualizzata la pianificazione dell'operazione, mentre se la modalità è impostata su un criterio, viene visualizzato il nome del criterio.

- Tipo di deduplicazione

Specifica il tipo di operazione di deduplicazione in esecuzione sul volume. Se il volume è in una relazione SnapVault, il tipo visualizzato è SnapVault. Per qualsiasi altro volume, il tipo viene visualizzato come Regolare.

- Politica di efficienza di archiviazione

Specifica il nome del criterio di efficienza di archiviazione assegnato tramite Unified Manager a questo volume. Questa policy può controllare le impostazioni di compressione e deduplicazione.

- **Protezione**

- Copie istantanee

Specifica se le copie automatiche degli snapshot sono abilitate o disabilitate.

Scheda di 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 viene selezionato un volume primario, vengono visualizzati solo i criteri di copia snapshot locale e gestita. Le proprietà visualizzate per le relazioni SnapMirror e SnapVault includono quanto segue:

- Volume sorgente

Visualizza il nome dell'origine del volume selezionato se il volume selezionato è una destinazione.

- Stato di ritardo

Visualizza lo stato di ritardo dell'aggiornamento o del trasferimento per una relazione di protezione. Lo stato può essere Errore, Avviso o Critico.

Lo stato di ritardo non è applicabile alle relazioni sincrone.

- Durata del ritardo

Visualizza il ritardo temporale dei dati sullo specchio rispetto alla sorgente.

- Ultimo aggiornamento riuscito

Visualizza la data e l'ora dell'ultimo aggiornamento di protezione riuscito.

L'ultimo aggiornamento riuscito non è applicabile alle relazioni sincrone.

- Membro del servizio di stoccaggio

Visualizza Sì o No per indicare se il volume appartiene o meno a un servizio di archiviazione ed è gestito da esso.

- Versione Replica Flessibile

Visualizza Sì, Sì con opzione di backup o Nessuno. Sì indica che la replica 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 di copie di backup sulla destinazione. Nessuno indica che la replica flessibile della versione non è abilitata.

- Capacità relazionale

Indica le capacità 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 partner di protezione.

- Tipo di relazione

Visualizza qualsiasi tipo di relazione, tra cui Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync e Sync.

- Stato della relazione

Visualizza lo stato della relazione SnapMirror o SnapVault . Lo stato può essere Non inizializzato, SnapMirrored o Interrotto. Se viene selezionato un volume sorgente, lo stato della relazione non è applicabile e non viene visualizzato.

- Stato del trasferimento

Visualizza lo stato del trasferimento per la relazione di protezione. Lo stato del trasferimento può essere uno dei seguenti:

- Aborto

I trasferimenti SnapMirror sono abilitati; tuttavia, è in corso un'operazione di interruzione del trasferimento che potrebbe includere la rimozione del checkpoint.

- Controllo

Il volume di destinazione è sottoposto a un controllo diagnostico e non è in corso alcun

trasferimento.

- Finalizzazione

I trasferimenti SnapMirror sono abilitati. Il volume è attualmente nella fase di post-trasferimento per trasferimenti incrementali SnapVault .

- Oziare

I trasferimenti sono abilitati e non è in corso alcun trasferimento.

- Sincronizzato

I dati nei due volumi nella relazione sincrona sono sincronizzati.

- Fuori sincrono

I dati nel volume di destinazione non sono sincronizzati con il volume di origine.

- Preparazione

I trasferimenti SnapMirror sono abilitati. Il volume è attualmente nella fase di pre-trasferimento per trasferimenti incrementali SnapVault .

- In coda

I trasferimenti SnapMirror sono abilitati. Non sono in corso trasferimenti.

- Quieced

I trasferimenti SnapMirror sono disabilitati. Nessun trasferimento in corso.

- Quiescenza

È in corso un trasferimento SnapMirror . I trasferimenti aggiuntivi sono disabilitati.

- Trasferimento

I trasferimenti SnapMirror sono abilitati e un trasferimento è in corso.

- Transizione

Il trasferimento asincrono dei dati dal volume di origine a quello di destinazione è completo e la transizione al funzionamento sincrono è iniziata.

- In attesa

È stato avviato un trasferimento SnapMirror , ma alcune attività associate sono in attesa di essere messe in coda.

- Velocità massima di trasferimento

Visualizza la velocità di trasferimento massima per la relazione. La velocità di trasferimento massima può essere un valore numerico espresso in kilobyte al secondo (Kbps), megabyte al secondo (Mbps), gigabyte al secondo (Gbps) o terabyte al secondo (Tbps). Se viene visualizzato Nessun limite, il trasferimento di base tra le relazioni è illimitato.

- **Politica SnapMirror**

Visualizza i criteri 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 predefinito Synchronous Strict, mentre Sync indica il criterio Synchronous predefinito. È possibile fare clic sul nome della policy per visualizzare i dettagli associati a tale policy, tra cui le seguenti informazioni:

- Priorità di trasferimento
- Ignora l'impostazione del tempo di accesso
- Limite di tentativi
- Commenti
- Etichette SnapMirror
- Impostazioni di conservazione
- Copie Snapshot effettive
- Conserva 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 dati (DP), si applica solo la regola "sm_created".

- **Aggiorna programma**

Visualizza la pianificazione SnapMirror assegnata alla relazione. Posizionando il cursore sull'icona informativa vengono visualizzati i dettagli della programmazione.

- **Criterio di snapshot locale**

Visualizza i criteri di copia snapshot per il volume. Il criterio può essere 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 di volume Consistency Group e SnapMirror, questo campo visualizza sia SnapMirror che Consistency Group. Questo campo fornisce anche un collegamento che reindirizza alla pagina Relazioni per visualizzare lo stato unificato della relazione. Il collegamento è applicabile solo alle relazioni costituenti.

- **Gruppo di coerenza**

Per i volumi protetti dalle relazioni di sincronizzazione attiva SnapMirror, questa colonna visualizza il gruppo di coerenza del volume.

- **Visualizzazioni**

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 doppie linee in grassetto specificano una relazione Asynchronous Mirror, una singola linea in grassetto specifica una relazione Asynchronous Vault, le doppie linee singole specificano una relazione Asynchronous MirrorVault e una linea in grassetto e una linea non in grassetto specificano 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, annullare, sospendere, interrompere, rimuovere o riprendere una relazione.

I menu non verranno visualizzati nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione, ad esempio se si dispone solo dei privilegi di operatore
- Se il volume è in una relazione di protezione sincrona
- Quando l'ID del volume è sconosciuto, ad esempio quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato rilevato, facendo clic su un altro volume nella topologia vengono selezionate e visualizzate le informazioni per quel 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 scoperto. Potrebbe anche indicare che mancano le informazioni sulla capacità. Posizionando il cursore sul punto interrogativo vengono visualizzate informazioni aggiuntive, tra cui suggerimenti per azioni correttive.

La topologia visualizza informazioni sulla capacità del volume, sul ritardo, sulle copie snapshot e sull'ultimo trasferimento dati riuscito, se conforme a uno dei numerosi 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 dati riuscito vengono visualizzate in una tabella delle relazioni sotto la topologia. In tal caso, la riga evidenziata nella tabella indica il volume selezionato e, nella vista topologica, le linee in grassetto con un punto blu indicano la relazione tra il volume selezionato e il suo volume sorgente.

Le viste topologiche 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 di soglia critica per quel volume nella finestra di dialogo Impostazioni soglia corrente. È anche possibile modificare le impostazioni della soglia facendo clic sul collegamento **Modifica soglie** nella finestra di dialogo Impostazioni soglia corrente. Deselezionando la casella di controllo **Capacità** vengono nascoste tutte le informazioni sulla capacità per tutti i volumi nella topologia.

- ritardo

Visualizza la durata e lo stato del ritardo delle relazioni di protezione in arrivo. Deselezionando la casella di controllo **Lag** vengono nascoste tutte le informazioni sul ritardo per tutti i volumi nella topologia. Quando la casella di controllo **Ritardo** è disattivata, le informazioni sul ritardo per il volume selezionato vengono visualizzate nella tabella delle relazioni sotto la topologia, insieme alle informazioni sul ritardo per tutti i volumi correlati.

- Istantanea

Visualizza il numero di copie Snapshot disponibili per un volume. Deselezionando la casella di controllo **Snapshot** vengono nascoste tutte le informazioni sulla copia Snapshot per tutti i volumi nella topologia.

Facendo clic sull'icona di copia Snapshot () visualizza l'elenco delle copie snapshot per un volume. Il conteggio delle copie Snapshot visualizzato accanto all'icona viene aggiornato circa ogni ora;

tuttavia, l'elenco delle copie Snapshot viene aggiornato nel momento in cui si fa clic sull'icona. Ciò potrebbe comportare una differenza tra il conteggio delle copie Snapshot visualizzato nella topologia e il numero di copie Snapshot elencate quando si fa clic sull'icona.

- **Ultimo trasferimento riuscito**

Visualizza l'importo, la durata, l'ora e la data dell'ultimo trasferimento dati riuscito. Quando la casella di controllo **Ultimo trasferimento riuscito** è disattivata, le informazioni sull'ultimo trasferimento riuscito per il volume selezionato vengono visualizzate nella tabella delle relazioni sotto la topologia, nonché 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 arrivo 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 da relazioni sincrone Consistency Group e SnapMirror, le informazioni sulla durata e sulle dimensioni del trasferimento della relazione non vengono visualizzate.

È possibile selezionare un tipo di grafico dall'elenco a discesa nella parte superiore del riquadro Cronologia. È anche possibile visualizzare i dettagli per un periodo di tempo specifico selezionando 1 settimana, 1 mese o 1 anno. I grafici cronologici possono aiutarti a identificare le tendenze: ad esempio, se grandi quantità di dati vengono trasferite nello stesso momento del giorno o della settimana, oppure se la soglia di avviso o errore di ritardo viene costantemente superata, puoi adottare le misure appropriate. Inoltre, puoi cliccare sul pulsante **Esporta** per creare un report in formato CSV per il grafico che stai visualizzando.

I grafici della cronologia della protezione mostrano le seguenti informazioni:

- **Durata del ritardo nella relazione**

Visualizza secondi, minuti o ore sull'asse verticale (y) e giorni, mesi o anni sull'asse orizzontale (x), a seconda del periodo di durata selezionato. Il valore superiore sull'asse y indica la durata massima del ritardo raggiunta nel periodo di durata mostrato sull'asse x. La linea orizzontale arancione sul grafico rappresenta la soglia di errore di ritardo, mentre la linea orizzontale gialla rappresenta la soglia di avviso di ritardo. Posizionando il cursore su queste linee viene visualizzata l'impostazione della soglia. La linea blu orizzontale indica la durata del ritardo. È possibile visualizzare i dettagli di punti specifici sul grafico posizionando il cursore su un'area di interesse.

- **Durata del trasferimento della relazione**

Visualizza secondi, minuti o ore sull'asse verticale (y) e giorni, mesi o anni sull'asse orizzontale (x), a seconda del periodo di durata selezionato. Il valore superiore sull'asse y indica la durata massima del trasferimento raggiunta nel periodo di durata mostrato 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 della relazione trasferita**

Visualizza byte, kilobyte, megabyte e così via sull'asse verticale (y), a seconda della dimensione 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 del trasferimento raggiunta nel periodo di durata mostrato sull'asse x. È possibile visualizzare i dettagli di punti specifici sul grafico posizionando il cursore su un'area di interesse.



Questo grafico non è disponibile per i volumi che si trovano in relazioni di protezione sincrona.

Area storica

L'area Cronologia visualizza grafici che forniscono informazioni sulla capacità e sulle prenotazioni di spazio del volume selezionato. Inoltre, puoi cliccare sul pulsante **Esporta** per creare un report in formato CSV per il grafico che stai visualizzando.

I grafici potrebbero essere vuoti e potrebbe essere visualizzato il messaggio Nessun dato trovato 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 anche possibile visualizzare i dettagli per un periodo di tempo specifico selezionando 1 settimana, 1 mese o 1 anno. I grafici cronologici possono aiutarti a identificare le tendenze: ad esempio, se l'utilizzo del volume supera costantemente la soglia "Quasi pieno", puoi adottare le misure appropriate.

I grafici cronologici mostrano le seguenti informazioni:

- **Capacità di 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 lineari in byte, kilobyte, megabyte e così via, sull'asse verticale (y). Il periodo di tempo è 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 sul 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 del volume, la linea del grafico Capacità utilizzata del volume viene nascosta.

- **Capacità di volume utilizzata rispetto al 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 del risparmio di spazio derivante dalla deduplicazione e dalla compressione, come grafici a linee, in byte, kilobyte, megabyte e così via, sull'asse verticale (y). Il periodo di tempo è 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 sul 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 volumetrica utilizzata (%)**

Visualizza la capacità utilizzata nel volume e l'andamento del modo in cui la capacità del volume viene utilizzata in base alla cronologia di utilizzo, come grafici a linee, in percentuale, sull'asse verticale (y). Il periodo di tempo è 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 sul 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 del volume, la linea

del grafico Capacità utilizzata del volume viene nascosta.

- **Capacità snapshot utilizzata (%)**

Visualizza la riserva Snapshot e la soglia di avviso Snapshot come grafici lineari e la capacità utilizzata dalle copie Snapshot come grafico ad area, in percentuale, sull'asse verticale (y). L'overflow dello Snapshot è rappresentato con colori diversi. Il periodo di tempo è 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 sul 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 mostra i dettagli sugli eventi nuovi e riconosciuti:

- **Gravità**

Visualizza la gravità 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 visualizzato il timestamp in cui è stato generato l'evento.

Riquadro 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 di annotazione applicati al volume. È anche possibile rimuovere le annotazioni manuali dal riquadro Annotazioni correlate.

Riquadro Dispositivi correlati

Il riquadro Dispositivi correlati consente di visualizzare e navigare tra gli SVM, gli aggregati, i qtree, i LUN e le copie Snapshot correlati al volume:

- **Macchina virtuale di archiviazione**

Visualizza la capacità e lo stato di integrità dell'SVM che contiene il volume selezionato.

- **Aggregato**

Visualizza la capacità e lo stato di integrità dell'aggregato che contiene il volume selezionato. Per i volumi FlexGroup, viene elencato 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 padre del volume selezionato. Viene visualizzato anche lo stato di integrità 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 i restanti cinque visualizzano lo stato Critico, lo stato visualizzato è Critico. Questo componente non viene

visualizzato per i volumi FlexGroup .

- **Qtrees**

Visualizza il numero di qtree contenuti nel volume selezionato e la capacità dei qtree con quota contenuti 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 gravità più elevato. Ad esempio, se un volume ha dieci qtree, cinque con stato di Avviso e i restanti cinque con stato Critico, lo stato visualizzato è Critico.

- **Azioni NFS**

Visualizza il numero e lo stato delle condivisioni NFS associate al volume.

- **Azioni SMB**

Visualizza il numero e lo stato delle condivisioni SMB/CIFS.

- **LUN**

Visualizza il numero e la dimensione totale di tutti i LUN nel volume selezionato. Viene visualizzato anche 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 gruppo utente 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 padre di un volume FlexClone selezionato. Il volume padre viene visualizzato solo se il volume selezionato è un volume FlexClone .

Riquadro Gruppi correlati

Il riquadro Gruppi correlati consente di visualizzare l'elenco dei gruppi associati al volume selezionato.

Riquadro Avvisi correlati

Il riquadro Avvisi correlati consente di visualizzare l'elenco degli avvisi creati per il volume selezionato. È anche possibile aggiungere un avviso cliccando sul link Aggiungi avviso oppure modificare un avviso esistente cliccando sul nome dell'avviso.

Pagina dei dettagli di Storage VM/Health

È possibile utilizzare la pagina Dettagli VM di archiviazione/Stato per visualizzare informazioni dettagliate sulla VM di archiviazione selezionata, ad esempio stato di integrità, capacità, configurazione, policy sui dati, interfacce logiche (LIF), LUN, qtree, utente, quote del gruppo utente e dettagli sulla protezione. È inoltre possibile visualizzare informazioni sugli oggetti correlati e sugli avvisi correlati per la VM di archiviazione.



È possibile monitorare solo la VM di archiviazione dati.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per la VM di archiviazione selezionata:

- **Passa alla visualizzazione delle prestazioni**

Consente di accedere alla pagina dei dettagli sulle prestazioni/VM di archiviazione.

- **Azioni**

- Aggiungi avviso

Consente di aggiungere un avviso alla VM di archiviazione selezionata.

- Annotare

Consente di annotare la VM di archiviazione selezionata.

- **Visualizza VM di archiviazione**

Consente di accedere alla vista Integrità: tutte le VM di archiviazione.

Scheda Salute

La scheda Integrità visualizza informazioni dettagliate sulla disponibilità dei dati, sulla capacità dei dati e sui problemi di protezione di vari oggetti quali 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 degli 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 gravità pari a un avviso.

- **Problemi di disponibilità**

Visualizza, sotto forma di grafico, il numero totale di oggetti, inclusi gli oggetti che presentano problemi di disponibilità e quelli 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 avuto un impatto sulla disponibilità dei dati nella VM di archiviazione. Ad esempio, vengono visualizzate informazioni sui LIF NAS e sui LIF SAN inattivi e sui volumi offline.

È inoltre possibile visualizzare informazioni sui protocolli e servizi correlati attualmente in esecuzione, nonché il numero e lo stato delle condivisioni NFS e CIFS.

- **Problemi di capacità**

Visualizza, sotto forma di grafico, il numero totale di oggetti, inclusi gli oggetti 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 avuto un impatto sulla capacità dei dati nella VM di archiviazione. Ad esempio, vengono visualizzate informazioni sugli aggregati che potrebbero superare i valori soglia impostati.

- **Problemi di protezione**

Fornisce una rapida panoramica dello stato di salute correlato alla protezione della VM di archiviazione visualizzando, come finestra di dialogo di campo, il numero totale di relazioni, incluse le relazioni che presentano problemi di protezione e quelle che non presentano problemi di protezione. È anche possibile visualizzare lo stato della relazione DR della VM di archiviazione per la VM di archiviazione selezionata. Qui vengono visualizzati gli eventi delle relazioni DR della VM di archiviazione; cliccando sugli eventi si accede alla pagina dei dettagli dell'evento. Se sono presenti volumi non protetti, facendo clic sul collegamento si accede alla vista Integrità: Tutti i volumi, in cui è possibile visualizzare un elenco filtrato dei volumi non protetti sulla VM di archiviazione. I colori nel grafico rappresentano i diversi livelli di gravità dei problemi. Facendo clic su un grafico si accede alla vista Relazione: Tutte le relazioni, in cui è possibile visualizzare un elenco filtrato dei dettagli della relazione di protezione. Le informazioni sotto il grafico forniscono dettagli sui problemi di protezione che possono avere un impatto o hanno già avuto un impatto sulla protezione dei dati nella VM di archiviazione. Ad esempio, vengono visualizzate informazioni sui volumi che hanno una riserva di copie Snapshot quasi piena o sui problemi di ritardo nella relazione SnapMirror .

Scheda Capacità

La scheda Capacità visualizza informazioni dettagliate sulla capacità dati dell'SVM selezionato.

Per una VM di archiviazione con FlexVol volume o volume FlexGroup vengono visualizzate le seguenti informazioni:

- **Capacità**

L'area Capacità mostra i dettagli sulla capacità utilizzata e disponibile allocata da tutti i volumi:

- Capacità totale

Visualizza la capacità totale della VM di archiviazione.

- Usato

Visualizza lo spazio utilizzato dai dati nei volumi che appartengono alla VM di archiviazione.

- Disponibilità garantita

Visualizza lo spazio garantito disponibile per i dati disponibili per i volumi nella VM di archiviazione.

- Non garantito

Visualizza lo spazio disponibile rimanente per i dati allocati per i volumi con provisioning ridotto nella VM di archiviazione.

- **Volumi con problemi di capacità**

L'elenco Volumi con problemi di capacità visualizza, in formato tabellare, i dettagli sui volumi che presentano problemi di capacità:

- Stato

Indica che il volume presenta un problema di capacità di gravità indicata.

È possibile spostare il puntatore sullo stato per visualizzare maggiori informazioni sull'evento o sugli

eventi correlati 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 l'evento è stato attivato, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. Puoi usare il pulsante **Visualizza dettagli** per visualizzare maggiori informazioni sull'evento.

Se lo stato del volume è determinato da più eventi della stessa gravità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data in cui sono stati attivati e il nome dell'amministratore a cui è assegnato l'evento. Puoi visualizzare maggiori dettagli su ciascuno di questi eventi cliccando sul nome dell'evento. Puoi anche cliccare sul link **Visualizza tutti gli eventi** per visualizzare l'elenco degli eventi generati.



Un volume può avere più eventi della stessa gravità o di gravità diversa. Tuttavia, viene visualizzata solo la gravità più elevata. Ad esempio, se un volume presenta due eventi con gravità Errore e Avviso, verrà visualizzata solo la gravità Errore.

- Volume

Visualizza il nome del volume.

- Capacità dati utilizzata

Visualizza, sotto forma di grafico, informazioni sull'utilizzo della capacità del volume (in percentuale).

- Giorni al completo

Visualizza il numero stimato di giorni rimanenti prima che il volume raggiunga la piena capacità.

- Fornito in modo sottile

Mostra se la garanzia di spazio è impostata per il volume selezionato. I valori validi sono Sì e No.

- Aggregati

Per i volumi FlexVol , visualizza il nome dell'aggregato che contiene il volume. Per i volumi FlexGroup , visualizza il numero di aggregati utilizzati nel FlexGroup.

Scheda di configurazione

La scheda Configurazione visualizza i dettagli di configurazione relativi alla VM di archiviazione selezionata, come il suo cluster, il volume radice, il tipo di volumi che contiene (volumi FlexVol), i criteri e la protezione creata sulla VM di archiviazione:

- **Panoramica**

- Grappolo

Visualizza il nome del cluster a cui appartiene la VM di archiviazione.

- Tipo di volume consentito

Visualizza il tipo di volumi che possono essere creati nella VM di archiviazione. Il tipo può essere FlexVol o FlexVol/ FlexGroup.

- Volume della radice

Visualizza il nome del volume radice della VM di archiviazione.

- Protocolli consentiti

Visualizza il tipo di protocolli che possono essere configurati sulla VM di archiviazione. Indica inoltre se un protocollo è attivo (●), giù (●), oppure non è configurato (●).

• Interfacce di rete dati

- NAS

Visualizza il numero di interfacce NAS associate alla VM di archiviazione. Indica inoltre se le interfacce sono attive (●) o verso il basso (●).

- SAN

Visualizza il numero di interfacce SAN associate alla VM di archiviazione. Indica inoltre se le interfacce sono attive (●) o verso il basso (●).

- FC-NVMe

Visualizza il numero di interfacce FC-NVMe associate alla VM di archiviazione. Indica inoltre se le interfacce sono attive (●) o verso il basso (●).

• Interfacce di rete di gestione

- Disponibilità

Visualizza il numero di interfacce di gestione associate alla VM di archiviazione. Indica inoltre se le interfacce di gestione sono attive (●) o verso il basso (●).

• Politiche

- Istantanee

Visualizza il nome del criterio Snapshot creato sulla VM di archiviazione.

- Politiche di esportazione

Visualizza il nome del criterio di esportazione se viene creato un singolo criterio oppure visualizza il numero di criteri di esportazione se vengono creati più criteri.

• Protezione

- VM di archiviazione DR

Visualizza se la VM di archiviazione selezionata è protetta, di destinazione o non protetta e il nome della destinazione in cui la VM di archiviazione è protetta. Se la VM di archiviazione selezionata è quella di destinazione, vengono visualizzati i dettagli della VM di archiviazione di origine. In caso di fan-out, questo campo visualizza il numero totale di VM di archiviazione di destinazione su cui è protetta la VM di archiviazione. Il collegamento di conteggio conduce alla griglia delle relazioni delle VM di archiviazione filtrata in base alla VM di archiviazione di origine.

- Volumi protetti

Visualizza il numero di volumi protetti sulla VM di archiviazione selezionata rispetto al totale dei volumi.

Se si visualizza una VM di archiviazione di destinazione, il collegamento numerico si riferisce ai volumi di destinazione della VM di archiviazione selezionata.

- Volumi non protetti

Visualizza il numero di volumi non protetti sulla VM di archiviazione selezionata.

- **Servizi**

- Tipo

Visualizza il tipo di servizio configurato sulla VM di archiviazione. Il tipo può essere Domain Name System (DNS) o Network Information Service (NIS).

- Stato

Visualizza lo stato del servizio, che può essere Su (🟢), Giù (🔴), o Non configurato (⚪).

- Nome di dominio

Visualizza i nomi di dominio completi (FQDN) del server DNS per i servizi DNS o del server NIS per i servizi NIS. Quando il server NIS è abilitato, viene visualizzato il nome di dominio completo (FQDN) attivo del server NIS. Quando il server NIS è disabilitato, viene visualizzato l'elenco di tutti gli FQDN.

- Indirizzo IP

Visualizza gli indirizzi IP del server DNS o NIS. Quando il server NIS è abilitato, viene visualizzato l'indirizzo IP attivo del server NIS. Quando il server NIS è disabilitato, viene visualizzato l'elenco di tutti gli indirizzi IP.

Scheda Interfacce di rete

La scheda Interfacce di rete visualizza i dettagli sulle interfacce di rete dati (LIF) create sulla VM di archiviazione selezionata:

- **Interfaccia di rete**

Visualizza il nome dell'interfaccia creata sulla VM di archiviazione 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 sue porte fisiche.

- **Stato amministrativo**

Visualizza lo stato amministrativo dell'interfaccia, che può essere Su (🟢), Giù (🔴), o Sconosciuto (🔵). Lo stato amministrativo di un'interfaccia è controllato dall'amministratore dell'archiviazione 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 è Inattivo, lo stato operativo è Inattivo per impostazione predefinita.

- **Indirizzo IP / WWPN**

Visualizza l'indirizzo IP per le interfacce Ethernet e il World Wide Port Name (WWPN) per i 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.

- **Porto di casa**

Visualizza la porta fisica a cui l'interfaccia era originariamente associata.

- **Porta corrente**

Visualizza la porta fisica a cui l'interfaccia è attualmente associata. Se l'interfaccia viene migrata, la porta corrente potrebbe essere diversa dalla porta home.

- **Porta impostata**

Visualizza il set di porte a cui è mappata l'interfaccia.

- **Criterio di failover**

Visualizza la policy di failover configurata per l'interfaccia. Per le interfacce NFS, CIFS e FlexCache, il criterio di failover predefinito è Next Available. La politica di failover non è applicabile alle interfacce FC e iSCSI.

- **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, pertanto per questi cluster viene visualizzata una colonna vuota.

- **Gruppo di failover**

Visualizza il nome del gruppo di failover.

Scheda Qtrees

La scheda Qtrees mostra i dettagli sui qtree e le relative quote. È possibile fare clic sul pulsante **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 **Esporta** per creare un file con valori separati da virgole (.csv) contenente i dettagli di tutti i qtree monitorati. Quando si esporta in un file CSV, è possibile scegliere di creare un report qtrees per la VM di archiviazione corrente, per tutte le VM di archiviazione nel cluster corrente o per tutte le VM di archiviazione per tutti i cluster nel data center. Nel file CSV esportato vengono visualizzati alcuni campi qtrees aggiuntivi.

- **Stato**

Visualizza lo stato corrente del qtree. Lo stato può essere Critico (❌), Errore (💡), Avvertimento (⚠️), o Normale (✅).

È possibile spostare il puntatore sull'icona di stato per visualizzare maggiori 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 l'evento è stato attivato, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. Puoi usare **Visualizza dettagli** per visualizzare maggiori informazioni sull'evento.

Se lo stato del qtree è determinato da più eventi della stessa gravità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data in cui sono stati attivati e il nome dell'amministratore a cui è assegnato l'evento. Puoi visualizzare maggiori dettagli su ciascuno di questi eventi cliccando sul nome dell'evento. Puoi anche usare **Visualizza tutti gli eventi** per visualizzare l'elenco degli eventi generati.



Un qtree può avere più eventi della stessa gravità o di gravità diversa. Tuttavia, viene visualizzata solo la gravità più elevata. Ad esempio, se un qtree ha due eventi con gravità Errore e Avviso, viene visualizzata solo la gravità Errore.

- **Qtree**

Visualizza il nome del qtree.

- **Grappolo**

Visualizza il nome del cluster contenente il qtree. Appare solo nel file CSV esportato.

- **Macchina virtuale di archiviazione**

Visualizza il nome della macchina virtuale di archiviazione (SVM) contenente il qtree. Appare 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 maggiori informazioni sul volume.

- **Impostazione della quota**

Indica se una quota è abilitata o disabilitata sul qtree.

- **Tipo di quota**

Specifica se la quota è per un utente, un gruppo di utenti o un qtree. Appare solo nel file CSV esportato.

- **Utente o gruppo**

Visualizza il nome dell'utente o del gruppo di utenti. Saranno presenti più righe per ogni utente e gruppo di utenti. Se il tipo di quota è qtree o se la quota non è impostata, la colonna è vuota. Appare solo nel file CSV esportato.

- **Disco utilizzato %**

Visualizza la percentuale di spazio su disco utilizzato. Se è impostato un limite rigido del disco, questo valore si basa sul limite rigido del disco. Se la quota è impostata senza un limite rigido del disco, il valore si

basa sullo spazio 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.

- **Limite massimo del disco**

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 sul disco. Il valore viene visualizzato come “Illimitato” nelle seguenti condizioni: se la quota è impostata senza un limite rigido del disco, se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree.

- **Limite software del disco**

Visualizza la quantità di spazio su disco allocato per il qtree prima che venga generato un evento di avviso. Il valore viene visualizzato come “Illimitato” nelle seguenti condizioni: se la quota è impostata senza un limite software 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.

- **Soglia del disco**

Visualizza il valore soglia impostato sullo spazio su disco. Il valore viene visualizzato come “Illimitato” nelle 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 è impostato il limite massimo del file, questo valore si basa sul limite massimo del file. Se la quota è impostata senza un limite rigido per i 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 di archiviazione**

Visualizza il limite massimo per il numero di file consentiti nei qtree. Il valore viene visualizzato come “Illimitato” nelle seguenti condizioni: se la quota è impostata senza un limite rigido per i file, se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree.

- **Limite flessibile del file**

Visualizza il limite flessibile per il numero di file consentiti nei qtree. Il valore viene visualizzato come “Illimitato” nelle seguenti condizioni: se la quota è impostata senza un limite software per i 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 sulle quote utente e gruppo utente per la VM di archiviazione selezionata. È possibile visualizzare informazioni quali lo stato della quota, il nome dell'utente o del gruppo di utenti, i limiti flessibili e rigidi impostati sui dischi e sui file, la quantità di spazio su disco e il numero di file utilizzati, nonché il valore della soglia del disco. È anche possibile modificare l'indirizzo email associato a un utente o a un gruppo di utenti.

- **Pulsante di comando Modifica indirizzo email**

Apri la finestra di dialogo Modifica indirizzo e-mail, che visualizza l'indirizzo e-mail corrente dell'utente o del gruppo di utenti selezionato. Puoi modificare l'indirizzo email. 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 regole per generare un indirizzo e-mail per le quote utente o gruppo utente configurate sulla VM di archiviazione. In caso di violazione della quota, viene inviata una notifica all'indirizzo e-mail specificato.

- **Stato**

Visualizza lo stato attuale della quota. Lo stato può essere Critico (❌), Avvertimento (⚠️), o Normale (✅).

È possibile spostare il puntatore sull'icona di stato per visualizzare maggiori 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 l'evento è stato attivato, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. Puoi usare **Visualizza dettagli** per visualizzare maggiori informazioni sull'evento.

Se lo stato della quota è determinato da più eventi della stessa gravità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data in cui sono stati attivati e il nome dell'amministratore a cui è assegnato l'evento. Puoi visualizzare maggiori dettagli su ciascuno di questi eventi cliccando sul nome dell'evento. Puoi anche usare **Visualizza tutti gli eventi** per visualizzare l'elenco degli eventi generati.



Una quota può avere più eventi della stessa gravità o di gravità diversa. Tuttavia, viene visualizzata solo la gravità più elevata. Ad esempio, se una quota ha due eventi con gravità Errore e Avviso, verrà visualizzata solo la gravità 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 su 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 rigido del disco.

- **Limite massimo del disco**

Visualizza la quantità massima di spazio su disco allocata per la quota. Unified Manager genera un evento critico quando viene raggiunto questo limite e non sono consentite ulteriori scritture sul disco. Il valore viene visualizzato come “Illimitato” se la quota è impostata senza un limite rigido del disco.

- **Limite software del disco**

Visualizza la quantità di spazio su disco allocata per la quota prima che venga generato un evento di avviso. Il valore viene visualizzato come “Illimitato” se la quota è impostata senza un limite software del disco. Per impostazione predefinita, questa colonna è nascosta.

- **Soglia del disco**

Visualizza il valore soglia impostato sullo spazio su disco. Il valore viene visualizzato come “Illimitato” 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 rigido per i file.

- **Limite massimo di archiviazione**

Visualizza il limite massimo per il numero di file consentiti nella quota. Il valore viene visualizzato come “Illimitato” se la quota è impostata senza un limite rigido per i file.

- **Limite flessibile del file**

Visualizza il limite flessibile per il numero di file consentiti nella quota. Il valore viene visualizzato come “Illimitato” se la quota è impostata senza un limite software per i file. Per impostazione predefinita, questa colonna è nascosta.

- **Indirizzo e-mail**

Visualizza l'indirizzo email 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 sulle condivisioni NFS, come lo 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. Le condivisioni NFS non verranno visualizzate nelle seguenti condizioni: se il volume non è montato o se i protocolli associati al criterio di esportazione per il volume non contengono condivisioni NFS.

- **Stato**

Visualizza lo stato corrente delle condivisioni NFS. Lo stato può essere Errore (❗) o Normale (✅).

- **Percorso di giunzione**

Visualizza il percorso in cui è montato il volume. Se a un qtree viene applicata una policy di esportazione NFS esplicita, la colonna visualizza il percorso del volume tramite 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 applicata la policy di esportazione NFS. Se un criterio di esportazione NFS viene applicato a un qtree nel volume, la colonna visualizza sia i nomi del volume sia del qtree.

È possibile fare clic sul collegamento per visualizzare i dettagli dell'oggetto nella rispettiva 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 viene esportato. Lo stato può essere Offline, Online, Limitato o Misto.

- Fuori linea

L'accesso in lettura o scrittura al volume non è consentito.

- In linea

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 sono tutti nello stesso stato.

- **Stile di sicurezza**

Visualizza l'autorizzazione di accesso per i volumi esportati. Lo stile di sicurezza può essere UNIX, Unificato, NTFS o Misto.

- UNIX (client NFS)

I file e le directory nel volume hanno autorizzazioni UNIX.

- Unificato

I file e le directory nel volume hanno uno stile di sicurezza unificato.

- NTFS (client CIFS)

I file e le directory nel volume hanno autorizzazioni Windows NTFS.

- Misto

I file e le directory nel volume possono avere autorizzazioni UNIX o autorizzazioni Windows NTFS.

- **Permesso UNIX**

Visualizza i bit di autorizzazione UNIX in un formato stringa ottale, impostato per i volumi esportati. È simile ai bit di autorizzazione in 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 alla policy di esportazione, ad esempio i protocolli di autenticazione e l'autorizzazione di accesso.

Scheda Condivisioni SMB

Visualizza informazioni sulle condivisioni SMB sulla VM di archiviazione selezionata. È possibile visualizzare informazioni quali lo stato della condivisione SMB, il nome della condivisione, il percorso associato alla VM di archiviazione, lo stato del percorso di giunzione della condivisione, l'oggetto contenitore, lo stato del volume contenitore, i dati di sicurezza della condivisione e i criteri di esportazione definiti per la condivisione. È anche 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 Visualizza mappatura utente**

Avvia la finestra di dialogo Mappatura utenti.

È possibile visualizzare i dettagli della mappatura degli utenti per la VM di archiviazione.

- **Mostra il pulsante di comando ACL**

Avvia la finestra di dialogo Controllo accessi 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 Errore (!).

- **Condividi nome**

Visualizza il nome della condivisione SMB.

- **Sentiero**

Visualizza il percorso di giunzione su cui è stata creata la condivisione.

- **Percorso di giunzione attivo**

Visualizza se il percorso per accedere alla condivisione è attivo o inattivo.

- **Oggetto contenente**

Visualizza il nome dell'oggetto contenitore a cui appartiene la condivisione. L'oggetto contenitore può essere un volume o un qtree.

Facendo clic sul collegamento, è possibile visualizzare i dettagli relativi all'oggetto contenitore nella rispettiva pagina Dettagli. Se l'oggetto contenitore è un qtree, vengono visualizzati i collegamenti sia per qtree che per volume.

- **Stato del volume**

Visualizza lo stato del volume che viene esportato. Lo stato può essere Offline, Online, Limitato o Misto.

- Fuori linea

L'accesso in lettura o scrittura al volume non è consentito.

- In linea

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 sono tutti nello stesso stato.

- **Sicurezza**

Visualizza l'autorizzazione di accesso per i volumi esportati. Lo stile di sicurezza può essere UNIX, Unificato, NTFS o Misto.

- UNIX (client NFS)

I file e le directory nel volume hanno autorizzazioni UNIX.

- Unificato

I file e le directory nel volume hanno uno stile di sicurezza unificato.

- NTFS (client CIFS)

I file e le directory nel volume hanno autorizzazioni Windows NTFS.

- Misto

I file e le directory nel volume possono avere autorizzazioni UNIX o autorizzazioni Windows NTFS.

- **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 archiviazione, il valore viene visualizzato come Non abilitato.

È possibile fare clic sul collegamento per visualizzare i dettagli sulle regole associate alla policy di esportazione, ad esempio i protocolli di accesso e le autorizzazioni. Il collegamento è disabilitato se il criterio di esportazione è disabilitato per la VM di archiviazione selezionata.

- **Equivalente NFS**

Specifica se esiste un equivalente NFS per la condivisione.

Scheda SAN

Visualizza i dettagli su LUN, gruppi di iniziatori e iniziatori per la VM di archiviazione selezionata. Per impostazione predefinita, viene visualizzata la vista LUN. È possibile visualizzare i dettagli sui gruppi di iniziatori nella scheda Gruppi di iniziatori e i dettagli sugli iniziatori nella scheda Iniziatori.

- **Scheda LUN**

Visualizza i dettagli sui LUN che appartengono alla VM di archiviazione selezionata. È possibile visualizzare informazioni quali il nome LUN, lo stato 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 Prestazioni LUN fornisce un collegamento alla pagina dei dettagli LUN/Prestazioni.

È inoltre possibile visualizzare informazioni per verificare se il thin provisioning è abilitato sulla LUN e se la LUN è mappata a un gruppo di iniziatori. Se è mappato a un iniziatore, è possibile visualizzare i gruppi di iniziatori e gli iniziatori mappati al LUN selezionato.

- **Scheda Gruppi Iniziatori**

Visualizza i dettagli sui gruppi iniziatori. È possibile visualizzare dettagli quali il nome del gruppo di iniziatori, 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 dello stato di accesso, è possibile visualizzare lo stato di accesso corrente del gruppo iniziatore.

- **Normale**

Il gruppo iniziatore è collegato a più percorsi di accesso.

- **Percorso singolo**

Il gruppo iniziatore è collegato a un singolo percorso di accesso.

- **Nessun percorso**

Non esiste alcun percorso di accesso collegato al gruppo iniziatore.

È possibile visualizzare se i gruppi di iniziatori sono mappati su tutte le interfacce o su interfacce specifiche tramite un set di porte. Facendo clic sul collegamento Conteggio nella colonna Interfacce mappate, vengono visualizzate tutte le interfacce oppure solo le interfacce specifiche per un set di porte. Le interfacce mappate tramite il portale di destinazione non vengono visualizzate. Viene visualizzato il numero totale di iniziatori e LUN mappati a un gruppo di iniziatori.

È anche possibile visualizzare i LUN e gli iniziatori mappati sul gruppo di iniziatori selezionato.

- **Scheda Iniziatori**

Visualizza il nome e il tipo dell'iniziatore e il numero totale di gruppi di iniziatori mappati a questo iniziatore

per la VM di archiviazione selezionata.

```
initiator groups that are mapped to the selected initiator group.
```

Riquadro Annotazioni correlate

Il riquadro Annotazioni correlate consente di visualizzare i dettagli delle annotazioni associati alla VM di archiviazione selezionata. I dettagli includono il nome dell'annotazione e i valori dell'annotazione applicati alla VM di archiviazione. È anche possibile rimuovere le annotazioni manuali dal riquadro Annotazioni correlate.

Riquadro Dispositivi correlati

Il riquadro Dispositivi correlati consente di visualizzare il cluster, gli aggregati e i volumi correlati alla VM di archiviazione:

- **Grappolo**

Visualizza lo stato di integrità del cluster a cui appartiene la VM di archiviazione.

- **Aggregati**

Visualizza il numero di aggregati che appartengono alla VM di archiviazione selezionata. Viene visualizzato anche lo stato di salute degli aggregati, in base al livello di gravità più elevato. Ad esempio, se una VM di archiviazione contiene dieci aggregati, cinque dei quali visualizzano lo stato Avviso e i restanti cinque visualizzano lo stato Critico, lo stato visualizzato è Critico.

- **Aggregati assegnati**

Visualizza il numero di aggregati assegnati a una VM di archiviazione. Viene visualizzato anche lo stato di salute degli aggregati, in base al livello di gravità più elevato.

- **Volumi**

Visualizza il numero e la capacità dei volumi che appartengono alla VM di archiviazione selezionata. Viene visualizzato anche lo stato di integrità dei volumi, in base al livello di gravità più elevato. Se nella VM di archiviazione sono presenti volumi FlexGroup, il conteggio include anche i FlexGroup, ma non i componenti FlexGroup.

Riquadro Gruppi correlati

Il riquadro Gruppi correlati consente di visualizzare l'elenco dei gruppi associati alla VM di archiviazione selezionata.

Riquadro Avvisi correlati

Il riquadro Avvisi correlati consente di visualizzare l'elenco degli avvisi creati per la VM di archiviazione selezionata. Puoi anche aggiungere un avviso cliccando sul link **Aggiungi avviso** oppure modificare un avviso esistente cliccando sul nome dell'avviso.

Pagina dei dettagli del cluster/salute

La pagina Dettagli cluster/stato 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), sui nodi, sui dischi, sui dispositivi correlati e sugli avvisi correlati per il cluster.

Lo stato accanto al nome del cluster, ad esempio (Buono), rappresenta lo stato della comunicazione, ovvero 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 prestazioni**

Consente di accedere alla pagina dei dettagli Cluster/Prestazioni.

- **Azioni**

- Aggiungi avviso: apre la finestra di dialogo 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 modifiche recenti apportate al cluster.

Se Unified Manager è abbinato a OnCommand Workflow Automation, l'operazione di riscoperta riacquisisce anche i dati memorizzati nella cache da WFA, se presenti.

Dopo l'avvio dell'operazione di riscoperta, viene visualizzato un collegamento ai dettagli del processo associato per consentire il monitoraggio dello stato del processo.

- Annota: consente di annotare il cluster selezionato.

- **Visualizza cluster**

Consente di passare alla vista Integrità: Tutti i cluster.

Scheda Salute

Visualizza informazioni dettagliate sulla disponibilità dei dati e sui problemi di capacità dei dati di vari oggetti del cluster, come nodi, SVM e aggregati. I problemi di disponibilità sono correlati alla capacità di elaborazione dei dati degli oggetti del cluster. I problemi di capacità sono correlati alla capacità di archiviazione 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 che hanno volumi o qtree con problemi di capacità con un livello di gravità di Avviso. È anche possibile fare clic sul grafico di 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 quelli 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 avuto un impatto sulla disponibilità dei dati nel cluster. Ad esempio, vengono

visualizzate informazioni sugli scaffali dei 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, compresi gli oggetti 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 riportate sotto il grafico forniscono dettagli sui problemi di capacità che possono avere un impatto o hanno già avuto un impatto sulla capacità dei dati nel cluster. Ad esempio, vengono visualizzate informazioni sugli aggregati che potrebbero superare i valori soglia impostati.

Scheda Capacità

Visualizza informazioni dettagliate sulla capacità del cluster selezionato.

Capacità

Visualizza il grafico della capacità dei dati relativa alla capacità utilizzata e alla capacità disponibile da tutti gli aggregati allocati:

- Spazio logico utilizzato

Le dimensioni reali dei dati archiviati su tutti gli aggregati di questo cluster senza applicare i risparmi derivanti dall'utilizzo delle tecnologie di efficienza di archiviazione ONTAP . Non sono incluse le copie Snapshot.

- Riduzione dei dati

Visualizza il rapporto senza copie Snapshot e con due cifre significative, ad esempio 1,8 a 1. Questo rapporto si basa sulle impostazioni di efficienza di archiviazione ONTAP configurate.

- Usato

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.

- Pezzi di ricambio

Visualizza la capacità di archiviazione disponibile in tutti i dischi di riserva.

- Fornito

Visualizza la capacità fornita per tutti i volumi sottostanti.

Dettagli

Visualizza informazioni dettagliate sulla capacità utilizzata e disponibile. Il calcolo esclude i dati aggregati della radice.

- Capacità totale

Visualizza la capacità totale del cluster. Ciò non include la capacità assegnata per la parità.

- Usato

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.

- Fornito

Visualizza la capacità fornita per tutti i volumi sottostanti.

- Pezzi di ricambio

Visualizza la capacità di archiviazione disponibile in tutti i dischi di riserva.

Livello cloud

Visualizza la capacità totale utilizzata del livello cloud e la capacità utilizzata per ciascun livello cloud connesso per gli aggregati abilitati per FabricPool sul cluster. Un FabricPool può essere concesso in licenza o meno.

Suddivisione della capacità fisica per tipo di disco

L'area Suddivisione della capacità fisica per tipo di disco visualizza informazioni dettagliate sulla capacità dei vari tipi di dischi nel cluster. Facendo clic sul tipo di disco, è possibile visualizzare ulteriori informazioni sul tipo di disco nella scheda 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 di archiviazione dei dischi cache SSD nel cluster.

- SSD di riserva

Visualizza graficamente la capacità inutilizzata dei dischi SSD, dati e cache nel cluster.

- Dischi non assegnati

Visualizza il numero di dischi non assegnati nel cluster.

Elenco degli aggregati con problemi di capacità

Visualizza in formato tabellare i dettagli sulla capacità utilizzata e sulla capacità disponibile degli aggregati che presentano problemi di rischio di capacità.

- Stato

Indica che l'aggregato presenta un problema di capacità di una certa gravità.

È possibile spostare il puntatore sullo stato per visualizzare maggiori 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 l'evento è stato attivato, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. Puoi cliccare sul pulsante **Visualizza dettagli** per visualizzare maggiori informazioni sull'evento.

Se lo stato dell'aggregato è determinato da più eventi della stessa gravità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data in cui vengono attivati gli eventi e il nome dell'amministratore a cui è assegnato l'evento. Puoi visualizzare maggiori dettagli su ciascuno di questi eventi cliccando sul nome dell'evento. Puoi anche cliccare sul link **Visualizza tutti gli eventi** per visualizzare l'elenco degli eventi generati.



Un aggregato può avere più eventi correlati alla capacità della stessa gravità o di gravità diversa. Tuttavia, viene visualizzata solo la gravità più elevata. Ad esempio, se un aggregato ha due eventi con livelli di gravità Errore e Critico, viene visualizzata solo la gravità Critica.

- Aggregato

Visualizza il nome dell'aggregato.

- Capacità dati utilizzata

Visualizza graficamente le informazioni sull'utilizzo della capacità aggregata (in percentuale).

- Giorni al completo

Visualizza il numero stimato di giorni rimanenti prima che l'aggregato raggiunga la piena capacità.

Scheda di configurazione

Visualizza i dettagli sul cluster selezionato, come indirizzo IP, contatto e posizione:

Panoramica del cluster

- Interfaccia di gestione

Visualizza il LIF di gestione del cluster utilizzato da Unified Manager per connettersi al cluster. Viene visualizzato anche lo stato operativo dell'interfaccia.

- Nome host o indirizzo IP

Visualizza il nome di dominio completo (FQDN), il nome breve o l'indirizzo IP del LIF di gestione del cluster utilizzato da Unified Manager per connettersi al cluster.

- Nome di dominio completo

Visualizza il nome di dominio completo (FQDN) del cluster.

- Versione OS

Visualizza la versione ONTAP in esecuzione sul cluster. Se i nodi nel cluster eseguono versioni diverse di ONTAP, verrà visualizzata la versione ONTAP meno recente.

- Contatto

Visualizza i dettagli sull'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 tutti gli array SAN.

Panoramica del cluster remoto

Fornisce dettagli sul cluster remoto in una configurazione MetroCluster . Queste informazioni vengono visualizzate solo per le configurazioni MetroCluster .

- Grappolo

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 il nome di dominio completo (FQDN), il nome breve o l'indirizzo IP del cluster remoto.

- Posizione

Visualizza la posizione del cluster remoto.

Panoramica MetroCluster

Fornisce dettagli sul cluster locale in una configurazione MetroCluster su FC o MetroCluster su IP. Queste informazioni vengono visualizzate solo per le configurazioni MetroCluster su FC o IP.

- Tipo

Visualizza se il tipo MetroCluster è a due o quattro nodi. Per MetroCluster su 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 di come è configurato il cluster)
 - Passaggio automatico non pianificato (AUSO)

Visualizza se il passaggio automatico non pianificato è abilitato 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 AUSO. Questa funzionalità è supportata solo per MetroCluster su FC.

- Modalità Switch-Over

Visualizza la modalità di commutazione per la configurazione MetroCluster su 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 ONTAP eseguite dai nodi, nonché il numero di nodi che eseguono una particolare 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 archiviazione

- Disponibilità

Visualizza il numero di SVM attivi (●) o verso il basso (●) nel cluster.

Interfacce di rete

- Disponibilità

Visualizza il numero di LIF non dati attivi (●) o verso il basso (●) nel cluster.

- Interfacce di gestione dei cluster

Visualizza il numero di LIF di gestione cluster.

- Interfacce di gestione dei nodi

Visualizza il numero di LIF di gestione dei nodi.

- Interfacce del cluster

Visualizza il numero di cluster LIF.

- Interfacce 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, in tal caso, 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 di 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 è irraggiungibile.

Livelli cloud

Elenca i nomi dei livelli cloud a cui è connesso questo cluster. Elenca anche il tipo (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage o StorageGRID) e gli stati dei livelli cloud (Disponibile o Non disponibile).

Scheda Connettività MetroCluster

Visualizza i problemi e lo stato di connettività dei componenti del cluster nella configurazione MetroCluster su FC. Un cluster viene visualizzato in un riquadro rosso quando il partner di disaster recovery del cluster presenta problemi.



La scheda Connettività MetroCluster viene visualizzata solo per i cluster che si trovano in una configurazione MetroCluster su FC.

È possibile accedere alla pagina dei dettagli di un cluster remoto facendo clic sul nome del cluster remoto. È anche possibile visualizzare i dettagli dei componenti cliccando sul collegamento del conteggio di un componente. Ad esempio, cliccando sul collegamento di conteggio del nodo nel cluster viene visualizzata la scheda del nodo nella pagina dei dettagli del cluster. Facendo clic sul collegamento del conteggio dei dischi nel cluster remoto viene visualizzata la scheda del disco nella pagina dei dettagli del cluster remoto.



Quando si gestisce una configurazione MetroCluster a otto nodi, facendo clic sul collegamento di conteggio del componente Disk Shelves vengono visualizzati solo gli shelf locali della coppia HA predefinita. Inoltre, non è possibile visualizzare gli scaffali 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 maggiori 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 quali il nome dell'evento, l'ora e la data in cui l'evento è stato attivato, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. Il pulsante Visualizza dettagli fornisce maggiori informazioni sull'evento.

Se lo stato del problema di connettività tra i componenti è determinato da più eventi della stessa gravità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data in cui vengono attivati gli eventi e il nome dell'amministratore a cui è assegnato l'evento. Puoi visualizzare maggiori dettagli su ciascuno di questi eventi cliccando sul nome dell'evento. Puoi anche cliccare sul link **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 peering. Un cluster viene visualizzato in un riquadro rosso quando il partner di disaster recovery del cluster presenta problemi.



La scheda Replica MetroCluster viene visualizzata solo per i cluster che si trovano in una configurazione MetroCluster su 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 oggettiva dei componenti del cluster con le relative connessioni logiche. Ciò aiuta a 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, mentre il partner MetroCluster fa riferimento al cluster remoto.

Scheda Interfacce di rete

Visualizza i dettagli su tutti i LIF non dati creati sul cluster selezionato.

Interfaccia di rete

Visualizza il nome del LIF creato 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 sue porte fisiche.

Stato amministrativo

Visualizza lo stato amministrativo dell'interfaccia, che può essere Su () , 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 un 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 di cluster e LIF intercluster.

Porto di casa

Visualizza la porta fisica a cui l'interfaccia era originariamente associata.

Porto attuale

Visualizza la porta fisica a cui l'interfaccia è attualmente associata. Dopo la migrazione LIF, la porta corrente potrebbe essere diversa dalla porta di casa.

Politica di failover

Visualizza la policy di failover configurata 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, pertanto per questi cluster viene visualizzata una colonna vuota.

Gruppo di failover

Visualizza il nome del gruppo di failover.

Scheda Nodi

Visualizza informazioni sui nodi nel cluster selezionato. È possibile visualizzare informazioni dettagliate sulle coppie HA, sugli scaffali dei 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 funzionante.

- **Giallo**

Il nodo ha preso il sopravvento sul nodo partner oppure sta riscontrando problemi ambientali.

- **Rosso**

Il nodo è inattivo.

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 acquisizione, viene visualizzato il seguente messaggio: Possibile failover dell'archiviazione.

È possibile visualizzare un elenco degli eventi correlati alla coppia HA e al suo ambiente, come ventole, alimentatori, batteria NVRAM , schede flash, processore di servizio e connettività degli scaffali dei dischi. È anche possibile visualizzare l'ora in cui sono stati attivati gli eventi.

È possibile visualizzare altre informazioni relative al nodo, come il numero di modello.

Se sono presenti cluster a nodo singolo, è anche possibile visualizzare i dettagli sui nodi.

Ripiani per dischi

Visualizza informazioni sugli scaffali dei dischi nella coppia HA.

È anche possibile visualizzare gli eventi generati per gli scaffali dei dischi e i componenti ambientali, nonché l'ora in cui gli eventi sono stati attivati.

- **ID scaffale**

Visualizza l'ID dello scaffale in cui si trova il disco.

- **Stato del componente**

Visualizza i dettagli ambientali degli scaffali dei dischi, come alimentatori, ventole, sensori di temperatura, sensori di corrente, connettività dei dischi e sensori di tensione. I dettagli ambientali vengono visualizzati come icone nei seguenti colori:

- **Verde**

I componenti ambientali funzionano correttamente.

- **Grigio**

Non sono disponibili dati per le componenti ambientali.

- **Rosso**

Alcuni componenti ambientali sono in calo.

- **Stato**

Visualizza lo stato dello scaffale del disco. Gli stati possibili sono Offline, Online, Nessuno stato, Inizializzazione richiesta, Mancante e Sconosciuto.

- **Modello**

Visualizza il numero di modello del ripiano del disco.

- **Scaffale del disco locale**

Indica se lo scaffale del disco si trova sul cluster locale o su quello remoto. Questa colonna viene visualizzata solo per i cluster in una configurazione MetroCluster .

- **ID univoco**

Visualizza l'identificatore univoco dello scaffale del disco.

- **Versione del firmware**

Visualizza la versione del firmware dello scaffale del disco.

porti

Visualizza informazioni sulle porte FC, FCoE ed Ethernet associate. È possibile visualizzare i dettagli sulle porte e sui LIF associati facendo clic sulle icone delle porte.

È anche 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 ed e0b.

- **Ruolo**

Visualizza il ruolo della porta. I ruoli possibili sono Cluster, Dati, Intercluster, Gestione nodi e Non definito.

- **Tipo**

Visualizza il protocollo del livello fisico utilizzato per la porta. I tipi possibili sono Ethernet, Fibre Channel e FCoE.

- **WWPN**

Visualizza il nome della porta in tutto il mondo (WWPN).

- **Firmware Rev**

Visualizza la revisione del firmware della porta FC/FCoE.

- **Stato**

Visualizza lo stato attuale della porta. Gli stati possibili sono Su, Giù, Collegamento non connesso o Sconosciuto (?).

È possibile visualizzare gli eventi relativi alla porta dall'elenco Eventi. È inoltre possibile visualizzare i

dettagli LIF associati, come il nome LIF, lo stato operativo, l'indirizzo IP o WWPN, i protocolli, il nome dell'SVM associato al LIF, la porta corrente, la policy di failover e il gruppo di failover.

Scheda Dischi

Visualizza i dettagli sui dischi nel cluster selezionato. È possibile visualizzare informazioni relative al disco, ad esempio il numero di dischi utilizzati, dischi di riserva, dischi danneggiati e dischi non assegnati. È possibile visualizzare anche altri dettagli, come 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, come il numero di aggregati, dischi condivisi, dischi di riserva, dischi danneggiati, dischi non assegnati e dischi non supportati. Facendo clic sul collegamento del conteggio effettivo del tipo di disco, vengono visualizzati i dischi con lo stato e il tipo effettivo selezionati. Ad esempio, se si fa clic sul collegamento di conteggio per lo stato del disco Interrotto e il tipo effettivo SAS, vengono visualizzati tutti i dischi con stato del disco Interrotto e 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, Di riserva, Interrotto, Non assegnato, Non supportato o Sconosciuto. Per impostazione predefinita, questa colonna è ordinata in modo da visualizzare gli stati nel seguente ordine: Interrotto, Non assegnato, Non supportato, Di riserva, Aggregato e Condiviso.

Disco locale

Visualizza Sì o No per indicare se il disco si trova sul cluster locale o su quello 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 impattati

Visualizza il numero di aggregati interessati dal guasto del disco. È possibile spostare il puntatore sul collegamento del conteggio per visualizzare gli aggregati interessati, quindi fare clic sul nome dell'aggregato per visualizzarne i dettagli. È anche possibile fare clic sul conteggio aggregato per visualizzare l'elenco degli aggregati interessati nella vista Salute: Tutti gli aggregati.

Nei seguenti casi non viene visualizzato alcun valore in questa colonna:

- Per i dischi danneggiati quando un cluster contenente tali dischi viene aggiunto a Unified Manager
- Quando non ci sono dischi guasti

Pool di archiviazione

Visualizza il nome del pool di archiviazione a cui appartiene l'SSD. È possibile spostare il puntatore sul nome del pool di archiviazione per visualizzarne i dettagli.

Capacità immagazzinabile

Visualizza la capacità del disco disponibile per l'uso.

Capacità grezza

Visualizza la capacità del disco grezzo 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 efficace

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 riserve. ONTAP assegna un tipo di disco effettivo a ciascun tipo di disco.

Blocchi di ricambio consumati %

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 dell'SSD utilizzata, in base all'utilizzo effettivo dell'SSD e alla previsione del produttore sulla durata dell'SSD. Un valore superiore a 99 indica che la resistenza stimata è stata esaurita, ma potrebbe non indicare un guasto dell'SSD. Se il valore è sconosciuto, il disco viene omesso.

Firmware

Visualizza la versione del firmware del disco.

giri al minuto

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.

Venditore

Visualizza il nome del fornitore del disco. Per impostazione predefinita, questa colonna è nascosta.

ID scaffale

Visualizza l'ID dello scaffale in cui si trova il disco.

Baia

Visualizza l'ID dell'alloggiamento in cui si trova il disco.

Riquadro 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 anche possibile rimuovere le annotazioni manuali dal riquadro Annotazioni correlate.

Riquadro Dispositivi correlati

Consente di visualizzare i dettagli del dispositivo associato al cluster selezionato.

I dettagli includono le proprietà del dispositivo connesso al cluster, come tipo, dimensione, conteggio e stato di integrità. È possibile fare clic sul collegamento del conteggio per un'analisi più approfondita su quel particolare dispositivo.

È possibile utilizzare il riquadro Partner MetroCluster per ottenere il conteggio e i dettagli sul partner MetroCluster remoto, insieme ai componenti del cluster associati, quali nodi, aggregati e SVM. Il riquadro Partner MetroCluster viene visualizzato solo per i cluster in una configurazione MetroCluster .

Il riquadro Dispositivi correlati consente di visualizzare e navigare tra i nodi, le SVM e gli aggregati correlati al cluster:

Partner MetroCluster

Visualizza lo stato di integrità del partner MetroCluster . Utilizzando il collegamento count, è possibile navigare ulteriormente e ottenere informazioni sullo stato di integrità e sulla capacità dei componenti del cluster.

Nodi

Visualizza il numero, la capacità e lo stato di integrità dei nodi che appartengono al cluster selezionato. La capacità indica la capacità totale utilizzabile rispetto alla capacità disponibile.

Macchine virtuali di archiviazione

Visualizza il numero di SVM appartenenti al cluster selezionato.

Aggregati

Visualizza il numero, la capacità e lo stato di integrità degli aggregati che appartengono al cluster selezionato.

Riquadro Gruppi correlati

Consente di visualizzare l'elenco dei gruppi che include il cluster selezionato.

Riquadro Avvisi correlati

Il riquadro Avvisi correlati consente di visualizzare l'elenco degli avvisi per il cluster selezionato. È anche possibile aggiungere un avviso cliccando sul link [Aggiungi avviso](#) oppure modificare un avviso esistente cliccando sul nome dell'avviso.

Informazioni correlate

["Pagina dei volumi"](#) ["Visualizzazione dell'elenco e dei dettagli dei cluster"](#)

Pagina dei dettagli aggregati/sanitari

È possibile utilizzare la pagina [Dettagli aggregato/integrità](#) per visualizzare informazioni dettagliate sull'aggregato selezionato, come capacità, informazioni sul disco, dettagli di configurazione ed eventi generati. È inoltre possibile visualizzare informazioni sugli oggetti correlati e sugli avvisi correlati per tale aggregato.

Pulsanti di comando



Durante il monitoraggio di un aggregato abilitato per FabricPool, i valori committed e overcommit in questa pagina sono rilevanti solo per la capacità locale o del livello di prestazioni. La quantità di spazio disponibile nel livello cloud non si riflette nei valori sovraimpegnati. Allo stesso modo, i valori soglia aggregati sono rilevanti solo per il livello di prestazioni locale.

I pulsanti di comando consentono di eseguire le seguenti attività per l'aggregato selezionato:

- **Passa alla visualizzazione delle prestazioni**

Consente di accedere alla pagina dei dettagli [Aggregati/Prestazioni](#).

- **Azioni**

- **Aggiungi avviso**

Consente di aggiungere un avviso all'aggregato selezionato.

- **Modifica soglie**

Consente di modificare le impostazioni della soglia per l'aggregato selezionato.

- **Visualizza aggregati**

Consente di passare alla vista [Salute: Tutti gli aggregati](#).

Scheda Capacità

La scheda [Capacità](#) visualizza informazioni dettagliate sull'aggregato selezionato, come la sua capacità, le soglie e il tasso di crescita giornaliero.

Per impostazione predefinita, gli eventi di capacità non vengono generati per gli aggregati radice. Inoltre, i valori soglia utilizzati da Unified Manager non sono applicabili agli aggregati radice del nodo. Solo un rappresentante del supporto tecnico può modificare le impostazioni per la generazione di questi eventi. Quando le impostazioni vengono modificate da un rappresentante del supporto tecnico, i valori di soglia vengono applicati all'aggregato radice del nodo.

• Capacità

Visualizza il grafico della capacità dei dati e il grafico delle copie snapshot, che mostrano i dettagli della capacità dell'aggregato:

- Spazio logico utilizzato

La dimensione reale dei dati memorizzati in forma aggregata, senza considerare i risparmi derivanti dall'utilizzo delle tecnologie di efficienza di archiviazione ONTAP .

- Usato

La capacità fisica utilizzata dai dati nell'aggregato.

- Troppo impegnato

Quando lo spazio nell'aggregato è sovraccaricato, il grafico visualizza un flag con la quantità sovraccaricata.

- Avvertimento

Visualizza una linea tratteggiata nel punto in cui è impostata la soglia di avviso, a indicare 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 nel punto in cui è impostata la soglia di errore, a indicare 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 zero.

Entrambi i grafici mostrano la capacità per cui la capacità Snapshot supera la riserva Snapshot se la capacità Snapshot utilizzata supera la riserva Snapshot.

• Livello Cloud

Visualizza lo spazio utilizzato dai dati nel livello cloud per gli aggregati abilitati per FabricPool. Un FabricPool può essere concesso in licenza o meno.

Quando il livello cloud viene replicato su un altro provider cloud (il "livello mirror"), entrambi i livelli cloud vengono visualizzati qui.

• Dettagli

Visualizza informazioni dettagliate sulla capacità.

- Capacità totale

Visualizza la capacità totale aggregata.

- Capacità dei dati

Visualizza la quantità di spazio utilizzata dall'aggregato (capacità utilizzata) e la quantità di spazio disponibile nell'aggregato (capacità libera).

- Riserva istantanea

Visualizza la capacità Snapshot utilizzata e libera dell'aggregato.

- Capacità sovraccaricata

Visualizza l'eccesso di impegno aggregato. L'overcommitment aggregato consente di fornire più spazio di archiviazione di quello effettivamente disponibile da un dato aggregato, a condizione che non tutto lo spazio di archiviazione sia attualmente utilizzato. Quando si utilizza il thin provisioning, la dimensione totale dei volumi nell'aggregato può superare la capacità totale dell'aggregato.



Se hai sovraccaricato il tuo aggregato, devi monitorare attentamente lo spazio disponibile e aggiungere spazio di archiviazione secondo necessità per evitare errori di scrittura dovuti a spazio insufficiente.

- Livello cloud

Visualizza lo spazio utilizzato dai dati nel livello cloud per gli aggregati abilitati per FabricPool. Un FabricPool può essere concesso in licenza o meno. Quando il livello cloud viene rispecchiato su un altro provider cloud (il livello mirror), entrambi i livelli cloud vengono visualizzati qui

- Spazio totale nella cache

Visualizza lo spazio totale delle unità a stato solido (SSD) o delle unità di allocazione aggiunte a un aggregato Flash Pool. Se hai abilitato Flash Pool per un aggregato ma non hai aggiunto alcun SSD, lo spazio della cache viene visualizzato come 0 KB.



Questo campo è nascosto se Flash Pool è disabilitato per un aggregato.

- Soglie aggregate

Visualizza le seguenti soglie di capacità aggregata:

- Soglia quasi piena

Specifica la percentuale in cui un aggregato è quasi pieno.

- Soglia completa

Specifica la percentuale in cui un aggregato è pieno.

- Soglia quasi superata

Specifica la percentuale in cui un aggregato è quasi sovraimpegnato.

- Soglia di impegno eccessivo

Specifica la percentuale in cui un aggregato è sovraimpegnato.

- 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 fuori

Visualizza il numero e la capacità dei volumi che vengono spostati fuori dall'aggregato.

È possibile fare clic sul collegamento per visualizzare ulteriori dettagli, ad esempio il nome del volume, l'aggregato in cui è stato spostato il volume, lo stato dell'operazione di spostamento del volume e l'ora di fine stimata.

- Volumi in

Visualizza il numero e la capacità residua dei volumi che vengono 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 stimata utilizzata dopo lo spostamento del volume

Visualizza la quantità stimata di spazio utilizzato (in percentuale e in KB, MB, GB e così via) in forma aggregata dopo il completamento delle operazioni di spostamento del volume.

- **Panoramica della capacità - Volumi**

Visualizza grafici che forniscono informazioni sulla capacità dei volumi contenuti nell'aggregato. Vengono visualizzate la quantità di spazio utilizzata dal volume (capacità utilizzata) e la quantità di spazio disponibile (capacità libera) nel volume. Quando viene generato l'evento Spazio a rischio del volume con thin provisioning per i volumi con thin provisioning, vengono visualizzate la quantità di spazio utilizzata dal volume (capacità utilizzata) e la quantità di spazio disponibile nel volume ma che non può essere utilizzata (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 la dimensione utilizzata, la dimensione fornita, 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 archiviazione (SVM) che contengono i volumi nell'aggregato. È anche possibile visualizzare i dettagli dei volumi con provisioning ridotto. 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 in forma aggregata.

Scheda Informazioni sul disco

Visualizza informazioni dettagliate sui dischi nell'aggregato selezionato, tra cui il tipo e la dimensione RAID e il tipo di dischi utilizzati nell'aggregato. La scheda visualizza anche graficamente i gruppi RAID e i tipi di dischi utilizzati (ad esempio SAS, ATA, FCAL, SSD o VMDISK). È possibile visualizzare ulteriori informazioni, come l'alloggiamento, lo scaffale e la velocità di rotazione del disco, posizionando il cursore sui dischi di parità e sui dischi dati.

- **Dati**

Visualizza graficamente i dettagli sui dischi dati dedicati, sui dischi dati condivisi o su 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 sia dei dischi dati dedicati sia di quelli 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 del gruppo**

Visualizza il numero massimo di dischi consentiti nel gruppo RAID.

- **Gruppi**

Visualizza il numero di gruppi RAID nell'aggregato.

- **Dischi utilizzati**

- **Tipo efficace**

Visualizza i tipi di dischi dati (ad esempio, ATA, SATA, FCAL, SSD o VMDISK) in forma aggregata.

- **Dischi 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 sui dischi condivisi vengono visualizzati solo quando l'aggregato contiene dischi condivisi.

- **Dischi di riserva**

Visualizza il tipo effettivo del disco, il numero e la capacità dei dischi dati di riserva disponibili per il nodo nell'aggregato selezionato.



Quando un aggregato viene sottoposto a failover sul 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 con cache dedicata:

- **Dettagli RAID**

- Tipo

Visualizza il tipo di RAID (RAID0, RAID4, RAID-DP o RAID-TEC).

- Dimensione del gruppo

Visualizza il numero massimo di dischi consentiti nel gruppo RAID.

- Gruppi

Visualizza il numero di gruppi RAID nell'aggregato.

- **Dischi utilizzati**

- Tipo efficace

Indica che i dischi utilizzati per la cache nell'aggregato sono di tipo SSD.

- Dischi 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 effettivo del disco, il numero e la capacità dei dischi di riserva disponibili per il nodo nell'aggregato selezionato per la cache.



Quando un aggregato viene sottoposto a failover sul 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 archiviazione**

Visualizza il nome del pool di archiviazione. È possibile spostare il puntatore sul nome del pool di archiviazione per visualizzare i seguenti dettagli:

- Stato

Visualizza lo stato del pool di archiviazione, che può essere integro o non integro.

- Assegnazioni totali

Visualizza le unità di allocazione totali e le dimensioni nel pool di archiviazione.

- Dimensione dell'unità di allocazione

Visualizza la quantità minima di spazio nel pool di archiviazione che può essere allocata a un aggregato.

- **Dischi**

Visualizza il numero di dischi utilizzati per creare il pool di archiviazione. Se il conteggio dei dischi nella colonna del pool di archiviazione e il numero di dischi visualizzati nella scheda Informazioni disco per quel pool di archiviazione non corrispondono, significa che uno o più dischi sono danneggiati e il pool di archiviazione non è integro.

- **Assegnazione utilizzata**

Visualizza il numero e la dimensione delle unità di allocazione utilizzate dagli aggregati. È possibile fare clic sul nome dell'aggregato per visualizzarne i dettagli.

- **Assegnazione disponibile**

Visualizza il numero e la dimensione delle unità di allocazione disponibili per i nodi. È possibile fare clic sul nome del nodo per visualizzare i dettagli aggregati.

- **Cache allocata**

Visualizza la dimensione 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 archiviazione.

- **Dettagli**

- **Pool di archiviazione**

Visualizza il numero di pool di archiviazione.

- **Dimensione totale**

Visualizza la dimensione totale dei pool di archiviazione.

- **Livello Cloud**

Visualizza il nome del livello cloud, se è stato configurato un aggregato abilitato per FabricPool, e mostra lo spazio totale utilizzato. Quando il livello cloud viene rispecchiato su un altro provider cloud (il livello mirror), i dettagli per entrambi i livelli cloud vengono visualizzati qui

Scheda di configurazione

La scheda Configurazione visualizza i dettagli sull'aggregato selezionato, come il nodo del cluster, il tipo di blocco, il tipo di RAID, la dimensione del RAID e il conteggio dei gruppi RAID:

- **Panoramica**

- **Nodo**

Visualizza il nome del nodo che contiene l'aggregato selezionato.

- Tipo di blocco

Visualizza il formato del blocco dell'aggregato: 32 bit o 64 bit.

- Tipo RAID

Visualizza il tipo di RAID (RAID0, RAID4, RAID-DP, RAID-TEC o RAID misto).

- Dimensioni RAID

Visualizza la dimensione del gruppo RAID.

- Gruppi RAID

Visualizza il numero di gruppi RAID nell'aggregato.

- Tipo SnapLock

Visualizza il tipo SnapLock dell'aggregato.

- **Livello Cloud**

Se si tratta di un aggregato abilitato per FabricPool, vengono visualizzati i dettagli per il livello cloud. Alcuni campi variano a seconda del fornitore di archiviazione. Quando il livello cloud viene replicato su un altro provider cloud (il "livello mirror"), entrambi i livelli cloud vengono visualizzati qui.

- Fornitore

Visualizza il nome del provider di archiviazione, 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 al momento della sua creazione da parte di ONTAP.

- Server

Visualizza il nome di dominio completo (FQDN) del livello cloud.

- Porta

La porta utilizzata per comunicare con il provider cloud.

- Chiave di accesso o account

Visualizza la chiave di accesso o l'account per il livello cloud.

- Nome del contenitore

Visualizza il nome del bucket o del contenitore del livello cloud.

- SSL

Mostra se la crittografia SSL è abilitata per il livello cloud.

Area storica

L'area Cronologia visualizza grafici che forniscono informazioni sulla capacità dell'aggregato selezionato. Inoltre, puoi cliccare sul pulsante **Esporta** per creare un report in formato CSV per il grafico che stai visualizzando.

È possibile selezionare un tipo di grafico dall'elenco a discesa nella parte superiore del riquadro Cronologia. È anche possibile visualizzare i dettagli per un periodo di tempo specifico selezionando 1 settimana, 1 mese o 1 anno. I grafici cronologici possono aiutarti a identificare le tendenze: ad esempio, se l'utilizzo aggregato supera costantemente la soglia "Quasi pieno", puoi adottare le misure appropriate.

I grafici cronologici mostrano le seguenti informazioni:

- **Capacità aggregata utilizzata (%)**

Visualizza la capacità utilizzata nell'aggregato e l'andamento del modo in cui la capacità aggregata viene utilizzata in base alla cronologia di utilizzo come grafici a linee, in percentuale, sull'asse verticale (y). Il periodo di tempo è 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 sul 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, nonché la capacità utilizzata e la capacità totale, sotto forma di grafici lineari, in byte, kilobyte, megabyte e così via, sull'asse verticale (y). Il periodo di tempo è 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 sul 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 quella impegnata (%)**

Visualizza l'andamento dell'utilizzo della capacità aggregata in base alla cronologia di utilizzo, nonché lo spazio impegnato sotto forma di grafici a linee, in percentuale, sull'asse verticale (y). Il periodo di tempo è 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 sul 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 linea del grafico Spazio impegnato viene nascosta.

Elenco degli eventi

L'elenco Eventi mostra i dettagli sugli eventi nuovi e riconosciuti:

- **Gravità**

Visualizza la gravità 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 visualizzato il timestamp del momento in cui è stato generato l'evento.

Riquadro Dispositivi correlati

Il riquadro Dispositivi correlati consente di visualizzare i nodi 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. La 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 cluster che contiene l'aggregato selezionato. Viene visualizzato anche lo stato di salute degli aggregati, in base al livello di gravità più elevato. Ad esempio, se un nodo del cluster contiene dieci aggregati, cinque dei quali visualizzano lo stato Avviso e i restanti cinque visualizzano lo stato Critico, lo stato visualizzato è Critico.

- **Volumi**

Visualizza il numero e la capacità dei volumi FlexVol e FlexGroup in forma aggregata; il numero non include i componenti FlexGroup. Viene visualizzato anche lo stato di integrità 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.

Riquadro Avvisi correlati

Il riquadro Avvisi correlati consente di visualizzare l'elenco degli avvisi creati per l'aggregato selezionato. È anche possibile aggiungere un avviso cliccando sul link Aggiungi avviso oppure modificare un avviso esistente cliccando sul nome dell'avviso.

Informazioni correlate

["Visualizzazione dei dettagli del pool di archiviazione"](#)

Proteggere e ripristinare i dati

Creare, monitorare e risolvere i problemi delle relazioni di protezione

Unified Manager consente di creare relazioni di protezione, di monitorare e risolvere i problemi di protezione mirror e di protezione del vault di backup dei dati archiviati nei cluster gestiti e di ripristinare i dati quando vengono sovrascritti o persi.

Tipi di protezione SnapMirror

A seconda dell'implementazione della topologia di archiviazione dati, Unified Manager consente di configurare più tipi di relazioni di protezione SnapMirror. Tutte le varianti di protezione SnapMirror offrono protezione di disaster recovery in caso di failover, ma offrono funzionalità diverse in termini di prestazioni, flessibilità delle versioni e protezione da più copie di backup.

Relazioni di protezione asincrone tradizionali SnapMirror

La protezione asincrona SnapMirror tradizionale fornisce protezione mirror di replicazione a blocchi tra i volumi di origine e di destinazione.

Nelle relazioni SnapMirror tradizionali, le operazioni di mirroring vengono eseguite più velocemente rispetto alle relazioni SnapMirror alternative, perché l'operazione di mirroring si basa sulla replicazione a blocchi. Tuttavia, la protezione SnapMirror tradizionale richiede che il volume di destinazione venga eseguito con la stessa versione secondaria del software ONTAP o con una successiva del volume di origine all'interno della stessa versione 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 SnapMirror con replica flessibile in base alla versione

La protezione asincrona SnapMirror con replica flessibile in base alla versione fornisce una protezione mirror di replica logica tra volumi di origine e di destinazione, anche se tali volumi sono in esecuzione con versioni diverse del software ONTAP 8.3 o successive (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 SnapMirror con replica flessibile in base alla versione, le operazioni di mirroring non vengono eseguite con la stessa rapidità delle relazioni SnapMirror tradizionali.

A causa dell'esecuzione più lenta, SnapMirror con protezione della replica flessibile in base alla versione non è adatto all'implementazione in nessuna delle seguenti circostanze:

- L'oggetto sorgente 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. (Ciò significa che la destinazione deve sempre contenere dati speculari e recuperabili che non siano più vecchi di due ore rispetto ai dati presenti nella sorgente.)

In entrambe le circostanze elencate, è richiesta l'esecuzione più rapida basata sulla replicazione a blocchi della protezione SnapMirror predefinita.

Protezione asincrona SnapMirror con replica flessibile in base alla versione e opzione di backup

La protezione asincrona SnapMirror con opzione di replica e backup flessibile in base alla versione fornisce protezione mirror tra volumi di origine e di destinazione e la possibilità di archiviare più copie dei dati mirror nella destinazione.

L'amministratore dell'archiviazione può specificare quali copie Snapshot vengono replicate dall'origine alla destinazione e può anche specificare per quanto tempo conservare tali copie nella destinazione, anche se vengono eliminate dall'origine.

Nelle relazioni SnapMirror con opzione di replica e backup flessibile in base alla versione, le operazioni di mirroring non vengono eseguite con la stessa rapidità delle relazioni SnapMirror tradizionali.

SnapMirror Unified Replication (mirror e vault)

La replica unificata SnapMirror consente di configurare il ripristino di emergenza e l'archiviazione sullo stesso volume di destinazione. Come con SnapMirror, la protezione dati unificata esegue un trasferimento di base la prima volta che la si richiama. Un trasferimento di base in base alla policy di protezione 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 dati unificata non include le copie Snapshot più vecchie nella baseline.

Protezione sincrona SnapMirror con sincronizzazione rigorosa

La protezione sincrona SnapMirror con sincronizzazione "strict" garantisce che i volumi primario e secondario siano sempre una copia fedele l'uno dell'altro. Se si verifica un errore di replica durante il tentativo di scrivere dati sul volume secondario, l'I/O del client sul volume primario viene interrotto.

Protezione sincrona SnapMirror con sincronizzazione regolare

La protezione sincrona SnapMirror con sincronizzazione "regolare" non richiede che il volume primario e quello secondario siano sempre una copia fedele l'uno dell'altro, garantendo così la disponibilità del volume primario. Se si verifica un errore di replica durante il tentativo di scrivere dati sul volume secondario, i volumi primario e secondario perdono la sincronizzazione e l'I/O del client continuerà sul volume primario.



Il pulsante Ripristina e i pulsanti Operazione relazione non sono disponibili quando si monitorano le relazioni di protezione sincrona dalla vista Integrità: tutti i volumi o dalla pagina Dettagli volume/integrità.

Sincronizzazione attiva SnapMirror

La funzionalità di sincronizzazione attiva SnapMirror è disponibile con ONTAP 9.8 e versioni successive e può essere utilizzata per proteggere le applicazioni con LUN, consentendo alle applicazioni di eseguire il failover in modo trasparente, garantendo la continuità aziendale in caso di disastro.

Consente di scoprire e monitorare le relazioni SnapMirror sincrone per i gruppi di coerenza (CG) disponibili su cluster e macchine virtuali di archiviazione da Unified Manager. SnapMirror ActiveSync è supportato su cluster AFF o cluster All SAN Array (ASA), in cui i cluster primario e secondario possono essere AFF o ASA. SnapMirror ActiveSync protegge le applicazioni con LUN iSCSI o FCP.

Quando si visualizzano i volumi e i LUN protetti dalla relazione di sincronizzazione attiva SnapMirror, è possibile ottenere una vista unificata per le relazioni di protezione, i gruppi di coerenza nell'inventario dei volumi, visualizzare la topologia di protezione per le relazioni dei gruppi di coerenza e visualizzare i dati storici per le relazioni dei gruppi di coerenza fino a un anno. È anche possibile scaricare il rapporto. È inoltre possibile

visualizzare il riepilogo delle relazioni del Consistency Group, cercare supporto per le relazioni del Consistency Group e ottenere informazioni sui volumi protetti dal Consistency Group.

Nella pagina Relazioni è inoltre possibile ordinare, filtrare ed estendere la protezione sugli oggetti di archiviazione di origine e di destinazione e sulle relative relazioni protette dal Gruppo di coerenza.

Per saperne di più sulla sincronizzazione attiva SnapMirror, fare riferimento a ["Documentazione ONTAP 9 per Snapmirror ActiveSync \(precedentemente SM-BC\)"](#).

Impostare le relazioni di protezione in Unified Manager

Per utilizzare Unified Manager e OnCommand Workflow Automation per impostare le relazioni SnapMirror e SnapVault e proteggere i dati, è necessario eseguire diversi passaggi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver stabilito relazioni peer tra due cluster o due macchine virtuali di archiviazione (SVM).
- OnCommand Workflow Automation deve essere integrato con Unified Manager:
 - ["Configurare OnCommand Workflow Automation"](#).
 - ["Verifica della memorizzazione nella cache della fonte dati di Unified Manager in Workflow Automation"](#).

Passi

1. A seconda del tipo di rapporto di protezione che si desidera creare, procedere in uno dei seguenti modi:
 - ["Crea una relazione di protezione SnapMirror"](#).
 - ["Crea una relazione di protezione SnapVault"](#).
2. Se si desidera creare una policy per la relazione, a seconda del tipo di relazione che si sta creando, procedere in uno dei seguenti modi:
 - ["Crea una policy SnapVault"](#).
 - ["Crea una policy SnapMirror"](#).
3. ["Crea una pianificazione SnapMirror o SnapVault"](#).

Configurare una connessione tra Workflow Automation e Unified Manager

È possibile configurare una connessione sicura tra OnCommand Workflow Automation (WFA) e Unified Manager. La connessione a Workflow Automation consente di utilizzare funzionalità di protezione quali i flussi di lavoro di configurazione di SnapMirror e SnapVault, nonché comandi per la gestione delle relazioni SnapMirror.

Prima di iniziare

- La versione installata di Workflow Automation deve essere 5.1.1P6 o successiva.



Il "pacchetto WFA per la gestione di Clustered Data ONTAP" è incluso in WFA 5.1.1P6, quindi non è necessario scaricare questo pacchetto da NetAppStorage Automation Store e installarlo separatamente sul server WFA, come era necessario in passato. ["Pacchetto WFA per la gestione 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 di utente Schema di integrazione.

- È necessario che ti venga assegnato il ruolo di Amministratore o di Architetto in Workflow Automation.
- 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 Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Automazione del flusso di lavoro**.
2. Nell'area **Utente database** della pagina **Automazione flusso di lavoro**, seleziona il nome e immetti la password per l'utente del database creato per supportare le connessioni tra Unified Manager e Workflow Automation.
3. Nell'area **Credenziali di automazione del flusso di lavoro** della pagina, immettere il nome host o l'indirizzo IP (IPv4 o IPv6), nonché il nome utente e la password per la configurazione di automazione del flusso di lavoro.

È necessario utilizzare la porta del server Unified Manager (porta 443).

4. Fare clic su **Salva**.
5. Se si utilizza un certificato autofirmato, fare clic su **Sì** per autorizzare il certificato di sicurezza.

Viene visualizzata la pagina Automazione del flusso di lavoro.

6. Fare clic su **Sì** per ricaricare l'interfaccia utente Web e aggiungere le funzionalità di automazione del flusso di lavoro.

Informazioni correlate

["Documentazione NetApp : OnCommand Workflow Automation \(versioni correnti\)"](#)

Verificare la memorizzazione nella cache della fonte dati di Unified Manager in Workflow Automation

È possibile determinare se la memorizzazione nella cache dell'origine dati di Unified Manager funziona correttamente verificando se l'acquisizione dell'origine dati è riuscita in Workflow Automation. È possibile farlo quando si integra Workflow Automation con Unified Manager per garantire che la funzionalità Workflow Automation sia disponibile dopo l'integrazione.

Prima di iniziare

Per eseguire questa attività, è necessario disporre del ruolo di Amministratore o di Architetto in Workflow Automation.

Passi

1. Dall'interfaccia utente di Workflow Automation, seleziona **Esecuzione > Origini dati**.
2. Fare clic con il pulsante destro del mouse sul nome dell'origine dati di Unified Manager, quindi selezionare **Acquisisci ora**.
3. Verificare che l'acquisizione abbia esito positivo senza errori.

Per garantire la corretta integrazione di Workflow Automation con Unified Manager, è necessario risolvere gli errori di acquisizione.

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 OnCommand Workflow Automation attualmente in esecuzione o pianificati siano arrestati.

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.

Rimuovere la configurazione 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 Workflow Automation.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale > Automazione del flusso di lavoro** nel menu Impostazioni a sinistra.
2. Nella pagina **Automazione del flusso di lavoro**, fare clic su **Rimuovi configurazione**.

Eseguire un failover e un failback della relazione di protezione

Quando un volume di origine nella relazione di protezione viene disabilitato a causa di un guasto hardware o di un disastro, è possibile utilizzare le funzionalità della relazione di protezione in Unified Manager per rendere la destinazione di protezione accessibile in lettura/scrittura ed eseguire il failover su tale volume finché l'origine non torna online; a quel punto, è possibile eseguire il failover sull'origine originale quando è disponibile per fornire dati.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Per eseguire questa operazione è necessario aver configurato OnCommand Workflow Automation .

Passi

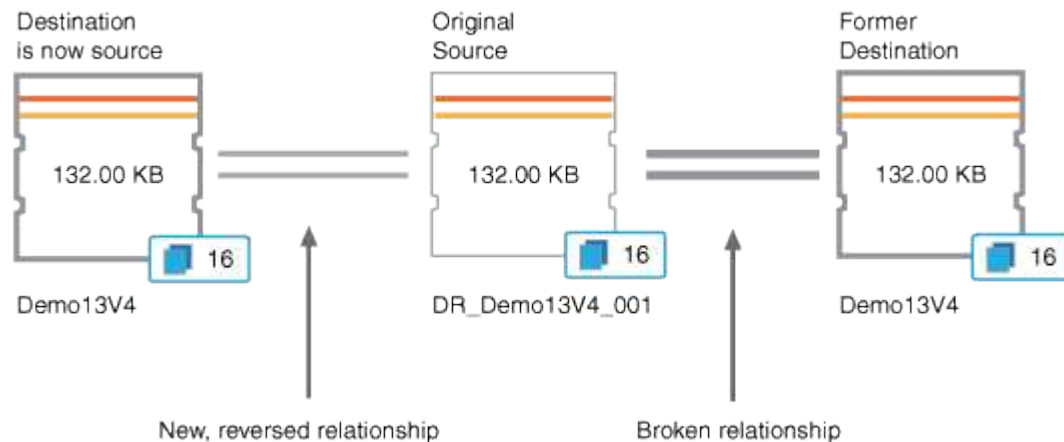
1. ["Interrompere la relazione SnapMirror"](#).

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 poter invertire la relazione.

2. ["Invertire il rapporto di protezione"](#).

Quando il volume sorgente originale sarà nuovamente disponibile, potresti decidere di ristabilire la relazione di protezione originale ripristinando il volume sorgente. Prima di poter ripristinare la sorgente, è necessario sincronizzarla con i dati scritti nella destinazione precedente. Utilizzare l'operazione di risincronizzazione inversa per 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 base per la nuova relazione.

La relazione invertita è simile a una relazione a cascata:



3. "Interrompere la relazione SnapMirror invertita".

Quando il volume sorgente originale viene risincronizzato e può nuovamente gestire i dati, utilizzare l'operazione di interruzione per interrompere la relazione invertita.

4. "Rimuovi la relazione".

Quando la relazione invertita non è più necessaria, è necessario rimuoverla 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.

Interrompere una relazione SnapMirror dalla pagina dei dettagli Volume/Stato

È possibile interrompere una relazione di protezione dalla pagina dei dettagli Volume/Stato e interrompere i trasferimenti di dati tra un volume di origine e uno di destinazione in una relazione SnapMirror. È possibile interrompere una relazione quando si desidera migrare dati, per il ripristino di emergenza o per testare un'applicazione. Il volume di destinazione viene modificato in un volume di lettura-scrittura. Non è possibile interrompere una relazione SnapVault.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, seleziona dalla topologia la relazione SnapMirror che desideri 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.

Relazioni di protezione inversa dalla pagina dei dettagli Volume/Salute

Quando un disastro disabilita il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per gestire i dati convertendoli in lettura/scrittura mentre si ripara o si sostituisce l'origine. Quando la sorgente è nuovamente disponibile per ricevere dati, è possibile utilizzare l'operazione di risincronizzazione inversa per stabilire la relazione nella direzione inversa, sincronizzando i dati sulla sorgente con i dati sulla destinazione di lettura/scrittura.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.
- La relazione non deve essere una relazione SnapVault .
- Deve già esistere un rapporto di protezione.
- Il rapporto di protezione deve essere interrotto.
- Sia la sorgente che la destinazione devono essere online.
- La sorgente non deve essere la destinazione di un altro volume di protezione dei dati.
- Quando si esegue questa attività, i dati sulla fonte più recenti rispetto ai dati sulla copia Snapshot comune vengono eliminati.
- Le policy e le pianificazioni create sulla relazione di risincronizzazione inversa sono le stesse di quelle sulla relazione di protezione originale.

Se non esistono policy e pianificazioni, vengono create.

Passi

1. Dalla scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, individuare nella topologia la relazione SnapMirror su cui si desidera invertire l'origine e la destinazione e fare clic con il pulsante destro del mouse.
2. Selezionare **Risincronizzazione inversa** dal menu.

Viene visualizzata la finestra di dialogo Risincronizzazione inversa.

3. Verificare che la relazione visualizzata nella finestra di dialogo **Risincronizzazione inversa** sia quella per cui si desidera eseguire l'operazione di risincronizzazione inversa, quindi fare clic su **Invia**.

La finestra di dialogo Risincronizzazione inversa viene chiusa e nella parte superiore della pagina Dettagli volume/integrità viene visualizzato un collegamento al processo.

4. **Facoltativo:** fare clic su **Visualizza processi** nella pagina dei dettagli **Volume/Stato** per monitorare lo stato di ciascun processo di risincronizzazione inversa.

Viene visualizzato un elenco filtrato di lavori.

5. **Facoltativo:** fai clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Salute**.

L'operazione di risincronizzazione inversa termina quando tutte le attività di lavoro sono state completate correttamente.

Rimuovere una relazione di protezione dalla pagina dei dettagli Volume/Salute

È possibile rimuovere una relazione di protezione per eliminare definitivamente 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.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, seleziona dalla topologia la relazione SnapMirror che desideri rimuovere.
2. Fare clic con il pulsante destro del mouse sul nome della destinazione e selezionare **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 dei dettagli Volume/Salute.

Risincronizzare le relazioni di protezione dalla pagina dei dettagli Volume/Stato

È possibile risincronizzare i dati su una relazione SnapMirror o SnapVault che è stata interrotta e in seguito la destinazione è stata resa di lettura/scrittura in modo che i dati sull'origine corrispondano ai dati sulla destinazione. È anche possibile risincronizzare quando una copia Snapshot comune richiesta sul volume di origine viene eliminata, causando il fallimento degli aggiornamenti di SnapMirror o SnapVault .

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato OnCommand Workflow Automation.

Passi

1. Dalla scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, individuare nella topologia la relazione di protezione che si desidera risincronizzare e fare clic con il pulsante destro del mouse.
2. Selezionare **Risincronizza** dal menu.

In alternativa, dal menu **Azioni**, seleziona **Relazione > Risincronizza** per risincronizzare la relazione di cui stai 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 **Copia snapshot di origine**; quindi, nella colonna **Copia snapshot**, fare clic su **Predefinito**.

Viene visualizzata la finestra di dialogo Seleziona copia snapshot di origine.

5. Se si desidera specificare una copia Snapshot esistente anziché trasferire la copia Snapshot predefinita, fare clic su **Copia Snapshot esistente** e selezionare una copia Snapshot dall'elenco.
6. Fare clic su **Invia**.

Verrà visualizzata nuovamente la finestra di dialogo Risincronizza.

7. Se hai selezionato più di una sorgente da risincronizzare, fai clic su **Predefinito** per la sorgente successiva per la quale desideri specificare una copia Snapshot esistente.
8. Fare clic su **Invia** per avviare il processo di risincronizzazione.

Il processo di risincronizzazione viene avviato, si torna alla pagina dei dettagli Volume/Stato e nella parte superiore della pagina viene visualizzato un collegamento ai processi.

9. **Facoltativo:** fare clic su **Visualizza processi** nella pagina **Dettagli volume/stato** per monitorare lo stato di ciascun processo di risincronizzazione.

Viene visualizzato un elenco filtrato di lavori.

10. **Facoltativo:** fai clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Salute**.

Il processo di risincronizzazione è terminato quando tutte le attività vengono completate correttamente.

Risolvere un errore del processo 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.

Prima di iniziare

Poiché alcune attività in questo flusso di lavoro richiedono l'accesso tramite il ruolo di Amministratore, è necessario avere familiarità con i ruoli richiesti per utilizzare varie funzionalità.

In questo scenario, accedi alla pagina Dashboard per verificare se ci sono problemi con i tuoi processi di protezione. Nell'area Incidente di protezione, si nota la presenza di un incidente Job terminato, che mostra un errore di errore di Job di protezione non riuscito su un volume. Esamina questo errore per determinarne la possibile causa e la possibile soluzione.

Passi

1. Nel pannello Incidenti di protezione dell'area Incidenti e rischi irrisolti della dashboard, fare clic sull'evento **Processo di protezione non riuscito**.



Il testo collegato all'evento è scritto nella forma `object_name:/object_name - Error Name`, ad esempio `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

Viene visualizzata la pagina dei dettagli dell'evento per il processo di protezione non riuscito.

2. Esaminare il messaggio di errore nel campo Causa dell'area **Riepilogo** per determinare il problema e valutare potenziali azioni correttive.

Vedere ["Identificazione del problema ed esecuzione di azioni correttive per un lavoro di protezione non riuscito"](#).

Identificare il problema ed eseguire azioni correttive per un lavoro di protezione non riuscito

Si esamina il messaggio di errore di errore del processo nel campo Causa nella pagina Dettagli evento e si determina che il processo non è riuscito a causa di un errore di copia snapshot. Si passa quindi alla pagina dei dettagli Volume/Salute per raccogliere maggiori informazioni.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Il messaggio di errore fornito nel campo Causa nella 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 prevedeva una relazione di protezione tra il volume sorgente `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 processo di copia snapshot non è riuscito per `0426cluster2_src_vol2snap` sul volume sorgente `cluster2_src_svm:/cluster2_src_vol2`.

In questo scenario è possibile identificare la causa e le potenziali azioni correttive dell'errore del processo. Tuttavia, per risolvere l'errore è necessario accedere all'interfaccia utente Web di System Manager o ai comandi ONTAP CLI.

Passi

1. Si esamina il messaggio di errore e si determina che un processo di copia snapshot non è riuscito sul volume di origine, il che indica che probabilmente c'è un problema con il volume di origine.

Facoltativamente, potresti cliccare sul link **Dettagli lavoro** alla fine del messaggio di errore, ma ai fini di questo scenario, scegli di non farlo.

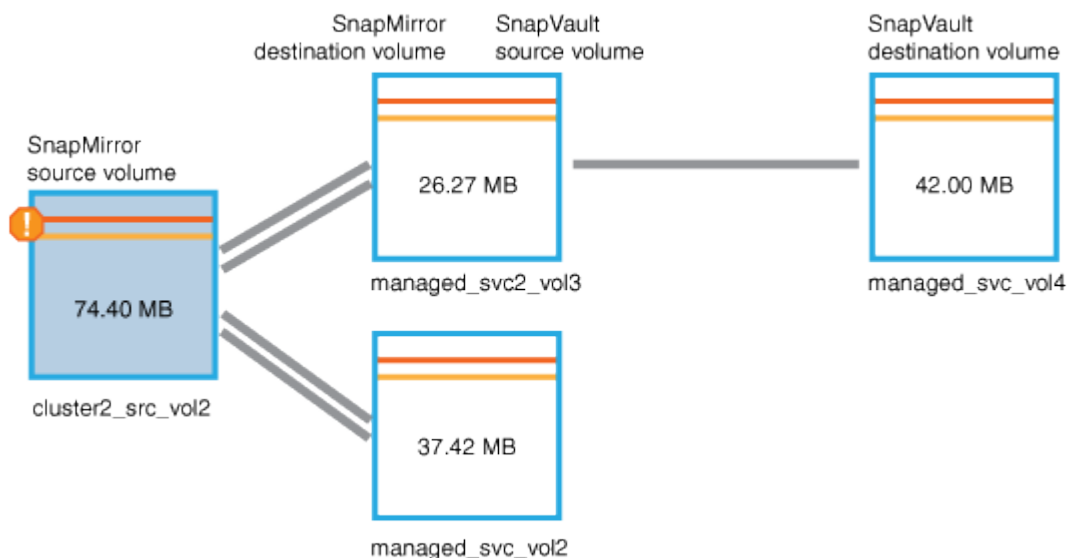
2. Decidi di provare a risolvere l'evento, quindi procedi come segue:
 - a. Fare clic sul pulsante **Assegna a** e selezionare **Io** dal menu.
 - b. Fare clic sul pulsante **Riconosci** per non continuare a ricevere notifiche di avviso ripetute, se sono stati impostati avvisi per l'evento.
 - c. Facoltativamente, puoi anche aggiungere delle note sull'evento.
3. Fare clic sul campo **Origine** nel riquadro **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 processo di copia Snapshot.

La pagina dei dettagli Volume/Salute viene visualizzata per `cluster2_src_vol2`, che mostra il contenuto della scheda Protezione.

4. Osservando il grafico della topologia di protezione, si nota un'icona di errore associata al primo volume nella topologia, che è il volume di origine per la relazione SnapMirror.

Sono visibili anche le barre orizzontali nell'icona del volume sorgente, che indicano le soglie di avviso e di errore impostate per quel volume.



5. Posizionando il cursore sull'icona di errore si apre la finestra di dialogo pop-up che mostra le impostazioni della soglia e si nota che il volume ha superato la soglia di errore, il che indica un problema di capacità.
6. Fare clic sulla scheda **Capacità**.

Informazioni sulla capacità del volume `cluster2_src_vol2` schermi.

7. Nel pannello **Capacità**, puoi vedere 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, puoi vedere che l'aumento automatico del volume è stato disabilitato e che è stata impostata una garanzia di spazio sul volume.

Potresti decidere di abilitare l'aumento automatico, ma ai fini di questo scenario, decidi di indagare ulteriormente prima di prendere una decisione su come risolvere il problema di capacità.

9. Scorrendo verso il basso fino all'elenco **Eventi** si noterà che sono stati generati gli eventi Protection Job Failed, Volume Days Until Full e Volume Space Full.
10. Nell'elenco **Eventi**, fai clic sull'evento **Spazio volume pieno** per ottenere maggiori informazioni, dopo aver deciso che questo evento sembra il più pertinente al tuo problema di capacità.

Nella pagina Dettagli evento viene visualizzato l'evento Spazio volume pieno per il volume di origine.

11. Nell'area **Riepilogo** puoi leggere 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 Riepilogo sono presenti le azioni correttive suggerite.



Le azioni correttive suggerite vengono visualizzate solo per alcuni eventi, pertanto quest'area non è visibile per tutti i tipi di eventi.

Fai clic sull'elenco delle azioni suggerite che potresti eseguire per risolvere l'evento Spazio volume pieno:

- Abilita l'aumento automatico su questo volume.
 - Ridimensiona il volume.
 - Abilita ed esegui la deduplicazione su questo volume.
 - Abilita ed esegui la compressione su questo volume.
13. Si decide di abilitare l'aumento automatico sul volume, ma per farlo è necessario determinare lo spazio libero disponibile sull'aggregato padre e l'attuale tasso di crescita del volume:
 - a. Guarda l'aggregato genitore, `cluster2_src_aggr1`, nel riquadro **Dispositivi correlati**.



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 l'aumento automatico del volume.

- b. Nella parte superiore della pagina, osserva l'icona che indica un incidente critico e leggi il testo sotto l'icona.

Si determina che "Giorni per il completamento: Meno di un giorno | Tasso di crescita giornaliero: 5,4%".

14. Vai a System Manager o accedi a ONTAP CLI per abilitare `volume autogrow` opzione.



Prendi nota dei nomi del volume e dell'aggregato in modo da averli a disposizione quando attivi l'aumento automatico.

15. Dopo aver risolto il problema di capacità, torna alla pagina dei dettagli **Evento** di Unified Manager e contrassegna l'evento come risolto.

Risolvere i problemi di ritardo

Questo flusso di lavoro fornisce un esempio di come risolvere un problema di ritardo. In questo scenario, sei un amministratore o un operatore che accede alla pagina Unified

ManagerDashboard per verificare se ci sono problemi con le tue relazioni di protezione e, in tal caso, per trovare soluzioni.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Nella pagina Dashboard, esaminando l'area Incidenti e rischi irrisolti, si nota un errore SnapMirror Lag nel riquadro Protezione in Rischi di protezione.

Passi

1. Nel riquadro **Protezione** nella pagina **Dashboard**, individua l'errore di ritardo della relazione SnapMirror e fai clic su di esso.

Viene visualizzata la pagina dei dettagli dell'evento di errore di ritardo.

2. Dalla pagina dei dettagli dell'**Evento** puoi eseguire una o più delle seguenti attività:

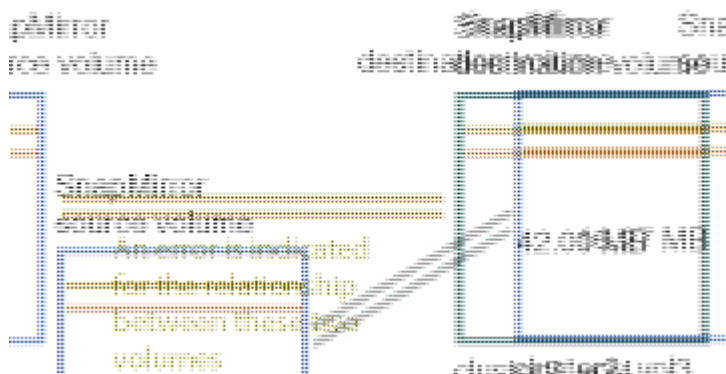
- Esaminare il messaggio di errore nel campo Causa dell'area Riepilogo per determinare se è possibile suggerire un'azione correttiva.
- Fare clic sul nome dell'oggetto, in questo caso un volume, nel campo Origine dell'area Riepilogo per ottenere dettagli sul volume.
- Cerca le note che potrebbero essere state aggiunte su questo evento.
- Aggiungi una nota all'evento.
- Assegna l'evento a un utente specifico.
- Riconoscere o risolvere l'evento.

3. In questo scenario, fai clic sul nome dell'oggetto (in questo caso, un volume) nel campo Origine dell'area **Riepilogo** per ottenere dettagli sul volume.

Viene visualizzata la scheda Protezione della pagina Dettagli volume/integrità.

4. Nella scheda **Protezione**, puoi osservare 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 è evidenziato in grigio scuro e una doppia linea arancione dal volume sorgente indica un errore di relazione SnapMirror.



5. Fare clic su ciascuno dei volumi nella cascata SnapMirror.

Selezionando ciascun volume, le informazioni sulla protezione nelle aree Riepilogo, Topologia, Cronologia, Eventi, Dispositivi correlati e Avvisi correlati cambiano per visualizzare i dettagli rilevanti per il volume.

selezionato.

6. Si guarda l'area **Riepilogo** e si posiziona il cursore sull'icona informativa nel campo **Aggiorna programma** per ciascun volume.

In questo scenario, si noti che il criterio SnapMirror è DPDefault e che la pianificazione SnapMirror si aggiorna ogni ora, cinque minuti dopo l'ora. Ti rendi conto che tutti i volumi nella relazione stanno tentando di completare un trasferimento SnapMirror contemporaneamente.

7. Per risolvere il problema del ritardo, è necessario modificare le pianificazioni per due dei volumi a cascata in modo che ogni destinazione avvii un trasferimento SnapMirror dopo che la sua origine ha completato un trasferimento.

Gestire e monitorare le relazioni di protezione

Active IQ Unified Manager consente di creare relazioni di protezione, di monitorare e risolvere i problemi delle relazioni SnapMirror e SnapVault sui cluster gestiti e di ripristinare i dati quando vengono sovrascritti o persi.

Per le operazioni SnapMirror esistono due tipi di replica:

- Asincrono

La replicazione dal volume primario a quello secondario è determinata da un programma.

- Sincrono

La replicazione viene eseguita simultaneamente sul volume primario e secondario.

È possibile eseguire fino a 10 attività di protezione contemporaneamente senza alcun impatto sulle prestazioni. Potresti riscontrare un impatto sulle prestazioni quando esegui contemporaneamente da 11 a 30 processi. Non è consigliabile eseguire più di 30 processi contemporaneamente.

Visualizza lo stato di protezione del volume

La pagina Protezione dati presenta una visione olistica dei dettagli sulla protezione dati per tutti i volumi protetti in un singolo cluster o per tutti i cluster in un data center.

Passi

1. Nel riquadro di navigazione a 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** oppure selezionare un singolo cluster dal menu a discesa.
3. Fare clic sulla freccia a destra nella parte superiore del pannello Protezione dati. Viene visualizzata la pagina **Protezione dei dati**.

A seconda che tu abbia selezionato un singolo cluster o tutti i cluster nel tuo data center, questa pagina visualizza lo stato di protezione dei dati dei volumi protetti da copie Snapshot o policy SnapMirror e mostra anche il conteggio dei volumi non protetti.

Selezionando un cluster dall'elenco **Cluster individuale** viene visualizzato lo stato della protezione Snapshot e della relazione SnapMirror dei volumi protetti in quel cluster.

Cliccando sugli eventi in questa pagina verrai indirizzato alla pagina dei dettagli dell'evento. È possibile fare clic sul collegamento **Visualizza tutto** per visualizzare tutti gli eventi di protezione attivi nella pagina dell'inventario Gestione eventi. È possibile passare il mouse per visualizzare i rispettivi conteggi e le relative legende. Puoi cliccare:

- I grafici a barre per i volumi non protetti e i volumi protetti da copie Snapshot consentono di accedere alla pagina Volumi e visualizzare i dettagli.
- I grafici a barre per tutte le relazioni portano alla pagina Relazioni, dove i dettagli vengono filtrati in base al cluster di origine.

Visualizza lo stato di protezione dei volumi protetti dalle copie Snapshot

Panoramica delle copie snapshot: una panoramica dei volumi protetti dalle copie snapshot, come:

- Numero totale di volumi protetti e non protetti da copie Snapshot.
- Numero totale di volumi che utilizzano o superano lo spazio di riserva per le copie Snapshot.

Analisi delle copie snapshot fornisce le seguenti informazioni:

- Eventi individuali 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.
- La ripartizione dei volumi avviene in base al numero delle relative copie Snapshot.

Punti da notare per le copie Snapshot

- Per il conteggio dei volumi protetti dalle copie Snapshot, vengono considerati sia i volumi di origine che quelli di destinazione.
- Il numero di copie Snapshot restituite si riferisce solo ai 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 abilitare la pianificazione per la copia Snapshot del volume.
- Il valore dello spazio di riserva 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.

Visualizza lo stato di protezione per le relazioni SnapMirror

- **Panoramica SnapMirror ***: una panoramica dei volumi protetti dalle policy SnapMirror , come:
- Numero di volumi protetti dalle rispettive policy SnapMirror , ad esempio relazioni SnapMirror dei volumi, ripristino di emergenza delle VM di archiviazione (SVM-DR) e relative combinazioni.
- Numero totale di relazioni SnapMirror che presentano un ritardo dell'obiettivo del punto di ripristino (RPO) in base allo stato del ritardo.
- L'analisi SnapMirror * fornisce le seguenti informazioni:
- Eventi individuali generati per le relazioni SnapMirror , inclusi gli eventi generati nelle ultime 24 ore
- Numero di volumi protetti da ciascun tipo di criterio SnapMirror .
- Numero di relazioni protette dai tipi di relazione SnapMirror , ad esempio Asynchronous Mirror,

Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, SnapMirror Active Sync Consistency Group e Sync.

- Il numero di relazioni sane e malsane.
- Scomposizione del conteggio della relazione di volume. È possibile alternare i grafici in base al tempo di ritardo e allo stato dell'RPO.
- Soglie di ritardo per relazioni non gestite. Puoi cliccare sull'icona delle impostazioni () per configurare le impostazioni della soglia di ritardo. Per maggiori informazioni, vedere ["Configurazione delle impostazioni della soglia di ritardo per le relazioni di protezione non gestite"](#).

Punti da notare per le relazioni SnapMirror

- Per il conteggio delle relazioni SnapMirror , vengono conteggiati i volumi di origine abilitati per la lettura e la scrittura. I volumi di destinazione e radice non vengono considerati.
- Per la relazione SnapMirror , gli eventi vengono visualizzati per il cluster di origine.
- Il conteggio delle relazioni SnapMirror include il numero di volumi con origini e destinazioni sullo stesso cluster o su cluster diversi.
- La durata del ritardo RPO nella replica dei dati si basa sulla relazione SnapMirror . Lo stato è classificato come `ok` , `warning` , `Warning` , `error` , in base alla soglia di relazione impostata. È possibile esaminare lo stato per determinare se i parametri funzionano come previsto o se è necessario risolvere qualche problema.
- Se un volume ha più relazioni SnapMirror , ogni tipo di relazione viene conteggiato per il ritardo RPO.
- Le relazioni tra volumi sono considerate non valide se si verificano problemi nella replicazione dei dati tra l'origine e la destinazione, ad esempio quando la relazione viene interrotta.

Visualizza i cluster protetti dalla configurazione MetroCluster

Il pannello **Protezione MetroCluster** * nella pagina **Protezione dati** mostra il numero di cluster protetti o non protetti da MetroCluster tramite configurazione FC o IP nel tuo sito. Facendo clic sui grafici a barre in questo pannello si accede alla pagina Cluster, in cui i dettagli dei cluster vengono filtrati in base ai cluster protetti o non protetti. Per informazioni sul monitoraggio della configurazione MetroCluster , vedere ["Monitoraggio delle configurazioni MetroCluster"](#) .

Visualizza le relazioni di protezione del volume

Dalla vista Relazione: Tutte le relazioni e dalla pagina Relazioni volume, è possibile visualizzare lo stato delle relazioni SnapMirror e SnapVault dei volumi esistenti. È inoltre possibile esaminare i dettagli sulle relazioni di protezione, tra cui lo stato di trasferimento e ritardo, i dettagli di origine e destinazione, le informazioni sulla pianificazione e sulla policy e così via.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Da questa pagina puoi anche avviare comandi di relazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Dal menu Visualizza, seleziona **Relazione > Tutte le relazioni**.

Viene visualizzata la vista Relazione: Tutte le relazioni.

3. Per visualizzare i dettagli sulla protezione del volume, scegliere uno dei seguenti metodi:

- Per visualizzare le informazioni correnti su tutte le relazioni di volume, rimanere sulla pagina predefinita **Tutte le relazioni**.
- Per visualizzare informazioni dettagliate sulle tendenze del trasferimento del volume in un determinato periodo di tempo, nel menu Visualizza, selezionare Relazione: visualizzazione Stato trasferimento ultimo mese.
- Per visualizzare informazioni dettagliate sull'attività di trasferimento del volume su base giornaliera, nel menu Visualizza, selezionare Relazione: visualizzazione Velocità di trasferimento ultimo mese.



Le viste di trasferimento del volume mostrano solo le informazioni sui volumi nelle relazioni asincrone; i volumi nelle relazioni sincrone non vengono mostrati.

Monitorare i LUN in una relazione di gruppo di coerenza

Se l'ambiente ONTAP supporta SnapMirror ActiveSync per proteggere le applicazioni con LUN, è possibile visualizzare e monitorare tali LUN su Active IQ Unified Manager.

La sincronizzazione attiva SnapMirror garantisce un RTO (Recovery Time Objective) pari a zero durante il failover negli ambienti SAN. In una tipica distribuzione che supporta la sincronizzazione attiva SnapMirror, le LUN sui volumi sono protette dalle relazioni Consistency Group.

Questi LUN primari e secondari sono LUN compositi, ovvero una coppia di LUN replica con lo stesso UUID e numero di serie. Le operazioni di I/O (sia di lettura che di scrittura) vengono multiplexate tra i siti di origine e di destinazione su queste LUN composite, garantendo la trasparenza.

Per visualizzare le LUN composite, è necessario aggiungere e rilevare su Unified Manager sia i cluster primari che quelli secondari con le LUN che fanno parte della relazione Consistency Group. Sono supportati solo i LUN iSCSI e FCP.

Per informazioni sulla sincronizzazione attiva SnapMirror, vedere ["Documentazione ONTAP 9 per SnapMirror ActiveSync \(precedentemente SM-BC\)"](#).

Per visualizzare le LUN composite nel tuo ambiente, segui questi passaggi:

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > LUN**.
2. Dal menu Visualizza, selezionare **Relazione > Tutti i LUN**.

Viene visualizzata la vista Relazione: tutti i LUN.

È possibile visualizzare i dettagli della LUN, come il nome della LUN, il volume, la VM di archiviazione che ospita la LUN, il cluster, il gruppo di coerenza e la LUN partner. È possibile fare clic su ciascuno di questi componenti per visualizzare una vista dettagliata. Facendo clic sul gruppo Coerenza si accede alla pagina Relazioni.

Facendo clic sulla LUN del partner è possibile visualizzarne i dettagli di configurazione nella scheda SAN della pagina Dettagli VM di archiviazione per la VM di archiviazione su cui è ospitata la LUN del partner. Vengono visualizzate informazioni quali gli iniziatori, i gruppi di iniziatori e altri aspetti del LUN partner.

È possibile eseguire le funzioni standard a livello di griglia di ordinamento, filtraggio, generazione e caricamento di report per le LUN protette nel proprio ambiente.

Creare una relazione di protezione SnapVault dalla vista Integrità: Tutti i volumi

È possibile utilizzare la vista Integrità: Tutti i volumi per creare relazioni SnapVault per uno o più volumi sulla stessa VM di archiviazione per abilitare i backup dei dati a scopo di protezione.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Il menu **Proteggi** non viene visualizzato nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione: ad esempio, se si dispone solo dei privilegi di operatore
- Quando l'ID del volume è sconosciuto: ad esempio, quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nella vista **Integrità: Tutti i volumi**, seleziona il volume che desideri proteggere e fai clic su **Proteggi**.

In alternativa, per creare più relazioni di protezione sulla stessa macchina virtuale di archiviazione (SVM), selezionare uno o più volumi nella vista Integrità: Tutti i volumi e fare clic su **Proteggi** sulla barra degli strumenti.

3. Seleziona * SnapVault* dal menu.

Viene aperta 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 **Avanzate** per impostare la deduplicazione, la compressione, l'aumento automatico e la garanzia dello spazio in base alle esigenze, quindi fare clic su **Applica**.
6. Completare l'area **Informazioni sulla destinazione** e l'area **Impostazioni relazione** nella scheda * SnapVault*.
7. Fare clic su **Applica**.

Verrai reindirizzato alla vista Salute: Tutti i volumi.

8. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della vista **Integrità: tutti i volumi**.

Se si sta creando una sola relazione di protezione, viene visualizzata la pagina Dettagli processo; se invece si stanno creando più relazioni di protezione, viene visualizzato un elenco filtrato di tutti i processi associati all'operazione di protezione.

9. Eseguire una delle seguenti operazioni:

- Se si dispone di un solo processo, fare clic su **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 completato.
- Se hai più di un lavoro:
 - i. Fare clic su un lavoro nell'elenco dei lavori.
 - ii. Fare clic su **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 completato.
 - iii. Utilizzare il pulsante **Indietro** per tornare all'elenco filtrato e visualizzare un altro lavoro.

Crea una relazione di protezione SnapVault dalla pagina dei dettagli Volume/Stato

È possibile creare una relazione SnapVault utilizzando la pagina Dettagli volume/integrità in modo che i backup dei dati siano abilitati per scopi di protezione sui volumi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Per eseguire questa attività è necessario aver configurato Workflow Automation.

Il menu **Proteggi** non viene visualizzato nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione: ad esempio, se si dispone solo dei privilegi di operatore
- Quando l'ID del volume è sconosciuto: ad esempio, quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, fare clic con il pulsante destro del mouse su un volume nella vista topologia che si desidera proteggere.
2. Selezionare **Proteggi** > * SnapVault* dal menu.

Viene aperta 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 **Avanzate** per impostare la deduplicazione, la compressione, l'aumento automatico e la garanzia dello spazio in base alle esigenze, quindi fare clic su **Applica**.
5. Completare l'area **Informazioni sulla destinazione** e l'area **Impostazioni relazione** nella finestra di dialogo **Configura protezione**.
6. Fare clic su **Applica**.

Verrai reindirizzato alla pagina dei dettagli Volume/Salute.

7. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Integrità**.

Viene visualizzata la pagina dei dettagli del lavoro.

8. Fare clic su **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 completato.

Una volta completate le attività di lavoro, le nuove relazioni vengono visualizzate nella vista topologica della pagina dei dettagli Volume/Stato.

Creare una relazione di protezione SnapMirror dalla vista Integrità: Tutti i volumi

Utilizzando la vista Integrità: tutti i volumi è possibile creare più relazioni di protezione SnapMirror contemporaneamente selezionando più volumi sulla stessa VM di archiviazione.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Il menu **Proteggi** non viene visualizzato nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione: ad esempio, se si dispone solo dei privilegi di operatore
- Quando l'ID del volume è sconosciuto: ad esempio, quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto

Passi

1. Nella vista **Integrità: Tutti i volumi**, seleziona il volume che desideri proteggere.

In alternativa, per creare più relazioni di protezione sullo stesso SVM, selezionare uno o più volumi nella vista Integrità: Tutti i volumi e fare clic su **Proteggi** > * SnapMirror* sulla 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 sulla destinazione.
3. Fare clic su **Avanzate** per impostare la garanzia di spazio, se necessario, quindi fare clic su **Applica**.
4. Completare l'area **Informazioni sulla destinazione** e l'area **Impostazioni relazione** nella scheda * SnapMirror*.
5. Fare clic su **Applica**.

Verrai reindirizzato alla vista Salute: Tutti i volumi.

6. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della vista **Integrità: tutti i volumi**.

Se si sta creando una sola relazione di protezione, viene visualizzata la pagina Dettagli processo; se invece si stanno creando più relazioni di protezione, viene visualizzato un elenco di tutti i processi associati all'operazione di protezione.

7. Eseguire una delle seguenti operazioni:
 - Se si dispone di un solo processo, fare clic su **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 completato.
 - Se hai più di un lavoro:

- i. Fare clic su un lavoro nell'elenco dei lavori.
- ii. Fare clic su **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 completato.
- iii. Utilizzare il pulsante **Indietro** per tornare all'elenco filtrato e visualizzare un altro lavoro.

A seconda della SVM di destinazione specificata durante la configurazione o delle opzioni abilitate nelle impostazioni avanzate, la relazione SnapMirror risultante potrebbe essere una delle seguenti possibili varianti:

- Se è stata specificata una SVM di destinazione eseguita con la stessa versione di ONTAP o con una versione più recente rispetto a quella del volume di origine, il risultato predefinito è una relazione SnapMirror basata sulla replicazione a blocchi.
- Se è stata specificata una SVM di destinazione eseguita con la stessa versione di ONTAP o con una versione più recente rispetto a quella del volume di origine, ma è stata abilitata la replica flessibile in base alla versione nelle impostazioni avanzate, il risultato sarà una relazione SnapMirror con replica flessibile in base alla versione.
- Se è stata specificata una SVM di destinazione eseguita con una versione di ONTAP precedente a quella del volume di origine e la versione precedente supporta la replica flessibile in base alla versione, il risultato automatico sarà una relazione SnapMirror con replica flessibile in base alla versione.

Crea una relazione di protezione SnapMirror dalla pagina dei dettagli Volume/Stato

È possibile utilizzare la pagina Dettagli volume/integrità per creare una relazione SnapMirror in modo che la replica dei dati sia abilitata per scopi di protezione. La replica SnapMirror consente di ripristinare i dati dal volume di destinazione in caso di perdita di dati sul volume di origine.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Il menu **Proteggi** non viene visualizzato nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione: ad esempio, se si dispone solo dei privilegi di operatore
- Quando l'ID del volume è sconosciuto: ad esempio, quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto

È possibile eseguire fino a 10 attività di protezione contemporaneamente senza alcun impatto sulle prestazioni. Potresti riscontrare un impatto sulle prestazioni quando esegui contemporaneamente da 11 a 30 processi. Non è consigliabile eseguire più di 30 processi contemporaneamente.

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, fare clic con il pulsante destro del mouse nella vista topologia sul nome del volume che si desidera proteggere.
2. Selezionare **Proteggi** > * 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 sulla destinazione.

4. Fare clic su **Avanzate** per impostare la garanzia di spazio, se necessario, quindi fare clic su **Applica**.
5. Completare l'area **Informazioni sulla destinazione** e l'area **Impostazioni relazione** nella finestra di dialogo **Configura protezione**.
6. Fare clic su **Applica**.

Verrai reindirizzato alla pagina dei dettagli Volume/Salute.

7. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Integrità**.

Le attività e i dettagli del lavoro vengono visualizzati nella pagina Dettagli lavoro.

8. Nella pagina dei dettagli **Job**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al job di configurazione della protezione e per determinare quando il job è completato.
9. Una volta completate le attività lavorative, fare clic su **Indietro** nel browser per tornare alla pagina dei dettagli **Volume / Salute**.

La nuova relazione viene visualizzata nella vista topologica della pagina Dettagli volume/stato.

A seconda della SVM di destinazione specificata durante la configurazione o delle opzioni abilitate nelle impostazioni avanzate, la relazione SnapMirror risultante potrebbe essere una delle seguenti possibili varianti:

- Se è stata specificata una SVM di destinazione eseguita con la stessa versione di ONTAP o con una versione più recente rispetto a quella del volume di origine, il risultato predefinito è una relazione SnapMirror basata sulla replicazione a blocchi.
- Se è stata specificata una SVM di destinazione eseguita con la stessa versione di ONTAP o con una versione più recente rispetto a quella del volume di origine, ma è stata abilitata la replica flessibile in base alla versione nelle impostazioni avanzate, il risultato sarà una relazione SnapMirror con replica flessibile in base alla versione.
- Se è stata specificata una SVM di destinazione 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 in base alla versione, il risultato automatico sarà una relazione SnapMirror con replica flessibile in base alla versione.

Crea una relazione SnapMirror con replica flessibile in base alla versione

È possibile creare una relazione SnapMirror con replica flessibile in base alla versione. La replica flessibile in base alla versione consente di implementare la protezione SnapMirror anche se i volumi di origine e di destinazione vengono eseguiti con versioni diverse di ONTAP.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.
- Sia la SVM di origine che quella di destinazione devono avere una licenza SnapMirror abilitata.
- Le SVM di origine e di destinazione devono essere eseguite ciascuna su una versione del software ONTAP che supporti la replica flessibile in base alla versione.

SnapMirror con replica flessibile in base alla versione consente di implementare la protezione SnapMirror

anche in ambienti di archiviazione eterogenei in cui non tutti gli archivi vengono eseguiti con un'unica versione di ONTAP; tuttavia, le operazioni di mirroring eseguite con SnapMirror con replica flessibile in base alla versione non vengono eseguite con la stessa rapidità che avrebbero con la tradizionale replica a blocchi SnapMirror.

Passi

1. Visualizzare la finestra di dialogo **Configura protezione** per il volume che si desidera proteggere.
 - Se stai visualizzando la scheda Protezione della pagina Dettagli volume/integrità, fai clic con il pulsante destro del mouse nella vista topologia che contiene il nome del volume che desideri proteggere e seleziona **Proteggi** > * SnapMirror* dal menu.
 - Se si sta visualizzando la vista Integrità: Tutti i volumi, individuare il volume che si desidera proteggere e fare clic con il pulsante destro del mouse; quindi selezionare **Proteggi** > * 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 **Informazioni sulla destinazione** e l'area **Impostazioni relazione** nella finestra di dialogo **Configura protezione**.

Se si specifica una SVM di destinazione eseguita con una versione di ONTAP precedente a quella del volume di origine che si sta proteggendo e se tale versione precedente supporta la replica flessibile in base alla versione, questa attività configura automaticamente SnapMirror con la replica flessibile in base alla 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 in base alla versione, fare clic su **Avanzate** per abilitare la replica flessibile in base alla versione, quindi fare clic su **Applica**.

5. Fare clic su **Applica**.

Verrai reindirizzato alla pagina dei dettagli Volume/Salute.

6. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Integrità**.

Le attività e i dettagli dei lavori vengono visualizzati nella pagina Dettagli lavoro.

7. Nella pagina dei dettagli **Job**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al job di configurazione della protezione e per determinare quando il job è completato.
8. Una volta completate le attività lavorative, fare clic su **Indietro** nel browser per tornare alla pagina dei dettagli **Volume / Salute**.

La nuova relazione viene visualizzata nella vista topologica della pagina Dettagli volume/stato.

Crea relazioni SnapMirror con replica flessibile in base alla versione con opzione di backup

È possibile creare una relazione SnapMirror con funzionalità di replica flessibile in base alla versione e di backup. La funzionalità dell'opzione di backup consente di implementare la protezione SnapMirror e di conservare più versioni di copie di backup nella posizione di destinazione.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.
- Sia la SVM di origine che quella di destinazione devono avere una licenza SnapMirror abilitata.
- Sia la SVM di origine che quella di destinazione devono avere una licenza SnapVault abilitata.
- Le SVM di origine e di destinazione devono essere eseguite ciascuna su una versione del software ONTAP che supporti la replica flessibile in base alla versione.

Configurando SnapMirror con la funzionalità di backup è possibile proteggere i dati con le funzionalità di disaster recovery SnapMirror, come la capacità di failover del volume, e allo stesso tempo fornire funzionalità SnapVault, come la protezione da più copie di backup.

Passi

1. Visualizzare la finestra di dialogo **Configura protezione** per il volume che si desidera proteggere.
 - Se stai visualizzando la scheda Protezione della pagina Dettagli volume/integrità, fai clic con il pulsante destro del mouse nella vista topologia sul nome del volume che desideri proteggere e seleziona **Proteggi** > * SnapMirror* dal menu.
 - Se si sta visualizzando la vista Integrità: Tutti i volumi, individuare il volume che si desidera proteggere e fare clic con il pulsante destro del mouse; quindi selezionare **Proteggi** > * 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 **Informazioni sulla destinazione** e l'area **Impostazioni relazione** nella finestra di dialogo **Configura protezione**.
4. Fare clic su **Avanzate** per visualizzare la finestra di dialogo **Impostazioni di destinazione avanzate**.
5. Se la casella di controllo **Replica flessibile versione** non è già selezionata, selezionarla ora.
6. Selezionare la casella di controllo **Con opzione di backup** per abilitare la funzionalità di opzione di backup; quindi fare clic su **Applica**.
7. Fare clic su **Applica**.

Verrai reindirizzato alla pagina dei dettagli Volume/Salute.

8. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Integrità**.

Le attività e i dettagli dei lavori vengono visualizzati nella pagina Dettagli lavoro.

9. Nella pagina dei dettagli **Job**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al job di configurazione della protezione e per determinare quando il job è completato.
10. Una volta completate le attività lavorative, fare clic su **Indietro** nel browser per tornare alla pagina dei dettagli **Volume / Salute**.

La nuova relazione viene visualizzata nella vista topologica della pagina Dettagli volume/stato.

Configurare le impostazioni di efficienza della destinazione

È possibile configurare le impostazioni di efficienza della destinazione, quali deduplicazione, compressione, aumento automatico e garanzia dello spazio su una destinazione di protezione, utilizzando la finestra di dialogo Impostazioni di destinazione

avanzate. Utilizzare queste impostazioni quando si desidera massimizzare l'utilizzo dello spazio su un volume di destinazione o secondario.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per impostazione predefinita, le impostazioni di efficienza corrispondono a quelle del volume sorgente, ad eccezione delle impostazioni di compressione in una relazione SnapVault, che sono disabilitate per impostazione predefinita.

Passi

1. Fare clic sulla scheda * SnapMirror* o sulla scheda * SnapVault* nella finestra di dialogo **Configura protezione**, a seconda del tipo di relazione che si sta configurando.
2. Fare clic su **Avanzate** nell'area **Informazioni sulla destinazione**.

Si apre la finestra di dialogo Impostazioni avanzate destinazione.

3. Abilita o disabilita le impostazioni di efficienza per deduplicazione, compressione, aumento automatico e garanzia dello spazio, a seconda delle necessità.
4. Fare clic su **Applica** per salvare le selezioni e tornare alla finestra di dialogo **Configura protezione**.

Crea pianificazioni SnapMirror e SnapVault

È possibile creare pianificazioni SnapMirror e SnapVault di base o avanzate per abilitare i trasferimenti automatici di protezione dei dati su un volume di origine o primario, in modo che i trasferimenti avvengano più o meno frequentemente, a seconda della frequenza con cui i dati cambiano sui volumi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver già completato l'area Informazioni sulla destinazione nella finestra di dialogo Configura protezione.
- Per eseguire questa attività è necessario aver configurato Workflow Automation.

Passi

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 Crea pianificazione.

2. Nel campo **Nome pianificazione**, digita il nome che desideri assegnare alla pianificazione.
3. Seleziona una delle seguenti opzioni:
 - **Di base**

Seleziona se vuoi creare una programmazione di base in stile intervallo.

- **Avanzato**

Seleziona se vuoi creare una pianificazione in stile cron.

4. Fare clic su **Crea**.

La nuova pianificazione viene visualizzata nell'elenco a discesa Pianificazione SnapMirror o Pianificazione SnapVault .

Creare relazioni a cascata o a fanout 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 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, ovvero un contenitore che contiene più volumi, in modo da poterli gestire tutti come un'unica entità. È possibile visualizzare il gruppo di coerenza di sincronizzazione attiva SnapMirror e la relazione del gruppo di coerenza sincrona nella pagina Relazioni di Unified Manager.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Fare clic su **Protezione > Relazioni**. In alternativa, è possibile visualizzare le relazioni dalla pagina Dettagli volume.
2. Dalla pagina **Relazioni volume**, seleziona la relazione SnapMirror da cui desideri estendere la protezione.
3. Sulla barra delle azioni, fare clic su **Estendi protezione**.
4. Nel menu, seleziona **Da origine** o **Da destinazione**, a seconda che tu 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 può essere ottenuto dalla pagina Relazione unificata/Relazione volume e Dettagli volume/Salute.

6. Completare le informazioni come indicato nella finestra di dialogo **Configura protezione**.

Modificare le relazioni di protezione dalla pagina Relazioni volume

È possibile modificare le relazioni di protezione esistenti per cambiare la velocità di trasferimento massima, la politica 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, poiché i dati cambiano spesso.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

I volumi selezionati devono essere destinazioni di 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 .

Passi

1. Dalla pagina **Relazioni volume**, seleziona nell'elenco dei volumi uno o più volumi nella stessa SVM per i quali desideri modificare le impostazioni delle relazioni, quindi seleziona **Modifica** dalla barra degli strumenti.

Viene visualizzata la finestra di dialogo **Modifica relazione**.

2. Nella finestra di dialogo **Modifica relazione**, modificare la velocità di trasferimento massima, la politica di protezione o la pianificazione della protezione, in base alle esigenze.
3. Fare clic su **Applica**.

Le modifiche vengono applicate alle relazioni selezionate.

Modificare le relazioni di protezione dalla pagina **Dettagli volume/salute**

È possibile modificare le relazioni di protezione esistenti per cambiare la velocità di trasferimento massima corrente, la politica 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, poiché i dati cambiano spesso.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver installato e configurato Workflow Automation.

I volumi selezionati devono essere destinazioni di 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 .

Passi

1. Dalla scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, individuare nella topologia la relazione di protezione che si desidera modificare e fare clic con il pulsante destro del mouse.
2. Selezionare **Modifica** dal menu.

In alternativa, dal menu **Azioni**, seleziona **Relazione > Modifica** per modificare la relazione di cui stai visualizzando i dettagli.

Viene visualizzata la finestra di dialogo **Modifica relazione**.

3. Nella finestra di dialogo **Modifica relazione**, modificare la velocità di trasferimento massima, la politica di protezione o la pianificazione della protezione, in base alle esigenze.
4. Fare clic su **Applica**.

Le modifiche vengono applicate alle relazioni selezionate.

Creare una policy SnapMirror per massimizzare l'efficienza del trasferimento

È possibile creare un criterio SnapMirror per specificare la priorità di trasferimento SnapMirror per le relazioni di protezione. I criteri SnapMirror consentono di massimizzare l'efficienza del trasferimento dall'origine alla destinazione assegnando priorità in modo che i trasferimenti con priorità inferiore vengano pianificati per essere eseguiti dopo i trasferimenti con priorità normale.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.
- Questa attività presuppone che sia già stata completata l'area Informazioni sulla destinazione nella finestra di dialogo Configura protezione.

Passi

1. Dalla scheda * SnapMirror* della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea criterio** nell'area **Impostazioni relazione**.

Viene visualizzata la finestra di dialogo Crea criterio SnapMirror .

2. Nel campo **Nome policy**, digitare il nome che si desidera assegnare alla policy.
3. Nel campo **Priorità di trasferimento**, seleziona la priorità di trasferimento che desideri assegnare alla policy.
4. Nel campo **Commento**, inserisci un commento facoltativo per la policy.
5. Fare clic su **Crea**.

La nuova policy viene visualizzata nell'elenco a discesa Policy SnapMirror .

Crea una policy SnapVault per massimizzare l'efficienza del trasferimento

È possibile creare un nuovo criterio SnapVault per impostare la priorità per un trasferimento SnapVault . Si utilizzano policy per massimizzare l'efficienza dei trasferimenti dal primario al secondario in una relazione di protezione.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.
- È necessario aver già completato l'area Informazioni sulla destinazione nella finestra di dialogo Configura protezione.

Passi

1. Dalla scheda * SnapVault* della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea criterio** nell'area **Impostazioni relazione**.

Viene visualizzata la scheda SnapVault .

2. Nel campo **Nome policy**, digitare il nome che si desidera assegnare alla policy.

3. Nel campo **Priorità di trasferimento**, seleziona la priorità di trasferimento che desideri assegnare alla policy.
4. **Facoltativo:** nel campo **Commento**, inserisci un commento per la policy.
5. Nell'area **Etichetta di replica**, aggiungere o modificare un'etichetta di replica, se necessario.
6. Fare clic su **Crea**.

La nuova policy viene visualizzata nell'elenco a discesa Crea policy.

Annulla un trasferimento di protezione dati attivo dalla pagina Relazioni volume

È possibile annullare un trasferimento di protezione dati attivo quando si desidera interrompere una replica SnapMirror in corso. È anche possibile cancellare il checkpoint di riavvio per i trasferimenti successivi al trasferimento di base. È possibile annullare un trasferimento quando entra in conflitto con un'altra operazione, ad esempio uno spostamento di volume.



Non è possibile interrompere le relazioni tra volumi protette dal Gruppo di coerenza.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato 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 dei privilegi di operatore
- Quando l'ID del volume è sconosciuto: ad esempio, quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto

Non è possibile cancellare il checkpoint di riavvio per un trasferimento di base.

Passi

1. Per annullare 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 **Annulla**.

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 base, selezionare **Cancella 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. **Facoltativo:** fare clic sul collegamento **Visualizza dettagli** per andare alla pagina dei dettagli del **Lavoro** per ulteriori dettagli e per visualizzare l'avanzamento del lavoro.

Annulla un trasferimento di protezione dati attivo dalla pagina dei dettagli Volume/Stato

È possibile annullare un trasferimento di protezione dati attivo quando si desidera interrompere una replica SnapMirror in corso. È anche possibile cancellare il checkpoint di riavvio per un trasferimento se non si tratta di un trasferimento di base. È possibile annullare un trasferimento quando entra in conflitto con un'altra operazione, ad esempio uno spostamento di volume.



Non è possibile interrompere le relazioni tra volumi protette dal Gruppo di coerenza.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato 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 dei privilegi di operatore
- Quando l'ID del volume è sconosciuto: ad esempio, quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto

Non è possibile cancellare il checkpoint di riavvio per un trasferimento di base.

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, fare clic con il pulsante destro del mouse sulla relazione nella vista topologia per il trasferimento dati che si desidera interrompere e selezionare **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 base, selezionare **Cancella 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/integrità insieme a un collegamento ai dettagli del processo.

4. **Facoltativo:** fare clic sul collegamento **Visualizza dettagli** per andare alla pagina dei dettagli del **Lavoro** per ulteriori dettagli e per visualizzare l'avanzamento del lavoro.
5. Fare clic su ciascuna attività lavorativa per visualizzarne i dettagli.
6. Fare clic sulla freccia Indietro del browser per tornare alla pagina dei dettagli **Volume / Salute**.

L'operazione di interruzione termina quando tutte le attività del lavoro vengono completate correttamente.

Disattiva una relazione di protezione dalla pagina Relazioni di volume

Dalla pagina Relazioni volume è possibile disattivare una relazione di protezione per

impedire temporaneamente il trasferimento dei dati. È possibile disattivare una relazione quando si desidera creare una copia Snapshot di un volume di destinazione SnapMirror contenente un database e si desidera garantire che il suo contenuto sia stabile durante l'operazione di copia Snapshot.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

L'azione di quiescenza non viene visualizzata nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione; ad esempio, se si dispone solo di privilegi di operatore
- Quando l'ID del volume è sconosciuto; ad esempio, quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto
- Quando non hai associato Workflow Automation e Unified Manager

Passi

1. Per sospendere 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 **Sospendi**.

Viene visualizzata la finestra di dialogo Quiesce.

2. Fare clic su **Continua**.

Lo stato del processo di quiesce viene visualizzato nella parte superiore della pagina dei dettagli Volume/Integrità, insieme a un collegamento ai dettagli del processo.

3. Fare clic sul collegamento **Visualizza dettagli** per andare alla pagina dei dettagli del **Lavoro** per ulteriori dettagli e per conoscere lo stato di avanzamento del lavoro.
4. **Facoltativo:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni di volume**.

Il processo di quiesce termina quando tutte le attività sono state completate con successo.

Disattiva una relazione di protezione dalla pagina dei dettagli Volume/Salute

È possibile sospendere una relazione di protezione per impedire temporaneamente il trasferimento dei dati. È possibile disattivare una relazione quando si desidera creare una copia Snapshot di un volume di destinazione SnapMirror contenente un database e si desidera garantire che il suo contenuto sia stabile durante la copia Snapshot.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

L'azione di quiescenza non viene visualizzata nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione, ad esempio se si dispone solo dei privilegi di operatore

- Quando l'ID del volume è sconosciuto, ad esempio quando si ha una relazione intercluster e il cluster di destinazione non è ancora stato scoperto
- Quando non hai associato Workflow Automation e Unified Manager

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, fare clic con il pulsante destro del mouse sulla relazione nella vista topologia per la relazione di protezione che si desidera disattivare.
2. Selezionare **Quiesce** dal menu.
3. Fare clic su **Sì** per continuare.

Lo stato del processo di quiesce viene visualizzato nella parte superiore della pagina dei dettagli Volume/Integrità, insieme a un collegamento ai dettagli del processo.

4. Fare clic sul collegamento **Visualizza dettagli** per andare alla pagina dei dettagli del **Lavoro** per ulteriori dettagli e per conoscere lo stato di avanzamento del lavoro.
5. **Facoltativo:** fai clic sulla freccia Indietro del browser per tornare alla pagina dei dettagli **Volume / Salute**.

Il processo di quiesce termina quando tutte le attività sono state completate con successo.

Interrompere una relazione SnapMirror dalla pagina Relazioni volume

È possibile interrompere una relazione di protezione per 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 dati, per il ripristino di emergenza o per testare un'applicazione. Il volume di destinazione viene modificato in un volume di lettura/scrittura. Non è possibile interrompere una relazione SnapVault .

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Dalla pagina **Relazioni volume**, seleziona uno o più volumi con relazioni di protezione per i quali desideri interrompere i trasferimenti di dati e, sulla barra degli strumenti, fai clic su **Interrompi**.

Viene visualizzata la finestra di dialogo Interrompi relazione.

2. Fare clic su **Continua** per interrompere la relazione.
3. Nella pagina **Relazioni volume**, verificare nella colonna **Stato relazione** che la relazione sia interrotta.

La colonna Stato relazione è nascosta per impostazione predefinita, quindi potrebbe essere necessario selezionarla nell'elenco delle colonne mostra/nascondi  .

Rimuovere una relazione di protezione dalla pagina Relazioni di volume

Dalla pagina Relazioni volume è possibile rimuovere una relazione di protezione per eliminare definitivamente 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.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Dalla pagina **Relazioni volume**, seleziona uno o più volumi con le relazioni di protezione che desideri rimuovere e, sulla barra degli strumenti, fai 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.

Riprendi i trasferimenti pianificati su una relazione sospesa dalla pagina Relazioni di volume

Dopo aver sospeso una relazione per impedire che si verifichino trasferimenti pianificati, è possibile utilizzare **Riprendi** per riattivare i trasferimenti pianificati in modo che i dati sul volume di origine o primario siano protetti. I trasferimenti riprendono da un checkpoint, se presente, al successivo intervallo di trasferimento programmato.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

È possibile selezionare non più di 10 relazioni sospese su cui riprendere i trasferimenti.

Passi

1. Dalla pagina **Relazioni** del volume, seleziona uno o più volumi con relazioni inattive e, sulla barra degli strumenti, fai clic su **Riprendi**.

2. Nella finestra di dialogo **Riprendi**, fare clic su **Continua**.

Verrai reindirizzato alla pagina Relazioni tra volumi.

3. Per visualizzare le attività lavorative correlate e monitorarne l'avanzamento, fare clic sul collegamento al lavoro visualizzato nella parte superiore della pagina **Relazioni di volume**.

4. Eseguire una delle seguenti operazioni:

- Se viene visualizzato un solo processo, nella pagina Dettagli processo fare clic su **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 completato.
- Se viene visualizzato più di un lavoro,
 - i. Nella pagina Lavori, fai clic sul lavoro di cui desideri visualizzare i dettagli.
 - ii. Nella pagina Dettagli attività, fare clic su **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 completato. Una volta completati i lavori, i trasferimenti di dati vengono ripresi al successivo intervallo di trasferimento pianificato.

Riprendi i trasferimenti programmati su una relazione sospesa dalla pagina dei dettagli Volume/Salute

Dopo aver sospeso una relazione per impedire che si verifichino trasferimenti pianificati, è possibile utilizzare **Riprendi** nella pagina Dettagli volume/integrità per riattivare i trasferimenti pianificati in modo che i dati sul volume di origine o primario siano protetti. I trasferimenti riprendono da un checkpoint, se presente, al successivo intervallo di trasferimento programmato.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, fare clic con il pulsante destro del mouse nella vista topologia su una relazione inattiva che si desidera riprendere.

In alternativa, seleziona **Riprendi** dal menu **Azioni > Relazione**.

2. Nella finestra di dialogo **Riprendi**, fare clic su **Continua**.

Verrai reindirizzato alla pagina dei dettagli Volume/Salute.

3. Per visualizzare le attività lavorative correlate e monitorarne l'avanzamento, fare clic sul collegamento al lavoro visualizzato nella parte superiore della pagina dei dettagli **Volume / Salute**.
4. Nella pagina dei dettagli **Job**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al job di configurazione della protezione e per determinare quando il job è completato.

Una volta completati i lavori, i trasferimenti di dati vengono ripresi al successivo intervallo di trasferimento pianificato.

Inizializzare o aggiornare le relazioni di protezione dalla pagina Relazioni volume

Dalla pagina Relazioni volume è possibile eseguire un primo trasferimento di base su una nuova relazione di protezione oppure aggiornare una relazione se è già inizializzata e si desidera eseguire un aggiornamento incrementale manuale e non pianificato per effettuare il trasferimento immediato.



Non è possibile inizializzare o aggiornare i volumi protetti dai gruppi di coerenza.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato OnCommand Workflow Automation.

Passi

1. Dalla pagina **Relazioni volume**, fare clic con il pulsante destro del mouse su un volume e selezionare uno

o più volumi con le relazioni che si desidera aggiornare o inizializzare, quindi, sulla barra degli strumenti, fare clic su **Inizializza/Aggiorna**.

Viene visualizzata la finestra di dialogo **Inizializza/Aggiorna**.

2. Nella scheda **Opzioni di trasferimento**, seleziona una priorità di trasferimento e la velocità di trasferimento massima.
3. Fare clic su **Copia snapshot di origine**; quindi, nella colonna **Copia snapshot**, fare clic su **Predefinito**.

Viene visualizzata la finestra di dialogo Seleziona copia snapshot di origine.

4. Se si desidera specificare una copia Snapshot esistente anziché trasferire la copia Snapshot predefinita, fare clic su **Copia Snapshot esistente** e selezionare una copia Snapshot dall'elenco.
5. Fare clic su **Invia**.

Verrà visualizzata nuovamente la finestra di dialogo **Inizializza/Aggiorna**.

6. Se hai selezionato più di una sorgente da inizializzare o aggiornare, fai clic su **Predefinito** per la sorgente successiva per la quale desideri specificare una copia Snapshot esistente.
7. Fare clic su **Invia** per avviare il processo di inizializzazione o aggiornamento.

Viene avviato il processo di inizializzazione o aggiornamento, si torna alla pagina Relazioni volume e nella parte superiore della pagina viene visualizzato un collegamento ai processi.

8. **Facoltativo:** fare clic su **Visualizza processi** nella vista **Integrità: tutti i volumi** per monitorare lo stato di ciascun processo di inizializzazione o aggiornamento.

Viene visualizzato un elenco filtrato di lavori.

9. **Facoltativo:** clicca su ogni lavoro per visualizzarne i dettagli.
10. **Facoltativo:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni di volume**.

L'operazione di inizializzazione o aggiornamento è terminata quando tutte le attività sono state completate correttamente.

Inizializza o aggiorna le relazioni di protezione dalla pagina dei dettagli Volume/Stato

È possibile eseguire un primo trasferimento di base su una nuova relazione di protezione oppure 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.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato OnCommand Workflow Automation.

Passi

1. Dalla scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, 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**, seleziona **Relazione > Inizializza/Aggiorna** per inizializzare o aggiornare la relazione di cui stai visualizzando i dettagli.

Viene visualizzata la finestra di dialogo Inizializza/Aggiorna.

3. Nella scheda **Opzioni di trasferimento**, seleziona una priorità di trasferimento e la velocità di trasferimento massima.
4. Fare clic su **Copia snapshot di origine**; quindi, nella colonna **Copia snapshot**, fare clic su **Predefinito**.

Viene visualizzata la finestra di dialogo Seleziona copia snapshot di origine.

5. Se si desidera specificare una copia Snapshot esistente anziché trasferire la copia Snapshot predefinita, fare clic su **Copia Snapshot esistente** e selezionare una copia Snapshot dall'elenco.
6. Fare clic su **Invia**.

Verrà visualizzata nuovamente la finestra di dialogo Inizializza/Aggiorna.

7. Se hai selezionato più di una sorgente da inizializzare o aggiornare, fai clic su **Predefinito** per la successiva sorgente di lettura/scrittura per la quale desideri specificare una copia Snapshot esistente.

Non è possibile selezionare una copia Snapshot diversa per i volumi di protezione dati.

8. Fare clic su **Invia** per avviare il processo di inizializzazione o aggiornamento.

Viene avviato il processo di inizializzazione o aggiornamento, si torna alla pagina dei dettagli Volume/Stato e nella parte superiore della pagina viene visualizzato un collegamento ai processi.

9. **Facoltativo:** fare clic su **Visualizza processi** nella pagina dei dettagli **Volume/Stato** per monitorare lo stato di ciascun processo di inizializzazione o aggiornamento.

Viene visualizzato un elenco filtrato di lavori.

10. **Facoltativo:** clicca su ogni lavoro per visualizzarne i dettagli.
11. **Facoltativo:** fai clic sulla freccia Indietro del browser per tornare alla pagina dei dettagli **Volume / Salute**.

L'operazione di inizializzazione o aggiornamento è terminata quando tutte le attività di lavoro sono state completate correttamente.

Risincronizzare le relazioni di protezione dalla pagina Relazioni volume

Dalla pagina Relazioni volume è possibile risincronizzare una relazione per ripristinare un evento che ha disabilitato il volume di origine o quando si desidera modificare l'origine corrente in un volume diverso.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Dalla pagina **Relazioni volume**, selezionare uno o più volumi con relazioni inattive 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 **Copie snapshot di origine**; quindi, nella colonna **Copia snapshot**, fare clic su **Predefinito**.

Viene visualizzata la finestra di dialogo Seleziona copia snapshot di origine.

4. Se si desidera specificare una copia Snapshot esistente anziché trasferire la copia Snapshot predefinita, fare clic su **Copia Snapshot esistente** e selezionare una copia Snapshot dall'elenco.
5. Fare clic su **Invia**.

Verrà visualizzata nuovamente la finestra di dialogo Risincronizza.

6. Se hai selezionato più di una sorgente da risincronizzare, fai clic su **Predefinito** per la sorgente successiva per la quale desideri specificare una copia Snapshot esistente.
7. Fare clic su **Invia** per avviare il processo di risincronizzazione.

Il processo di risincronizzazione viene avviato, si torna alla pagina Relazioni volume e nella parte superiore della pagina viene visualizzato un collegamento ai processi.

8. **Facoltativo:** fare clic su **Visualizza processi** nella pagina **Relazioni volume** per monitorare lo stato di ciascun processo di risincronizzazione.

Viene visualizzato un elenco filtrato di lavori.

9. **Facoltativo:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni di volume**.

L'operazione di risincronizzazione termina quando tutte le attività di lavoro vengono completate correttamente.

Relazioni di protezione inversa dalla pagina Relazioni di volume

Quando un disastro disabilita il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per gestire i dati convertendolo in un volume di lettura/scrittura mentre si ripara o si sostituisce l'origine. Quando la sorgente è nuovamente disponibile per ricevere dati, è possibile utilizzare l'operazione di risincronizzazione inversa per stabilire la relazione nella direzione inversa, sincronizzando i dati sulla sorgente con i dati sulla destinazione di lettura/scrittura.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.
- La relazione non deve essere una relazione SnapVault.
- Deve già esistere un rapporto di protezione.

- Il rapporto di protezione deve essere interrotto.
- Sia la sorgente che la destinazione devono essere online.
- La sorgente non deve essere la destinazione di un altro volume di protezione dei dati.
- Quando si esegue questa attività, i dati sulla fonte più recenti rispetto ai dati sulla copia Snapshot comune vengono eliminati.
- Le policy e le pianificazioni create sulle relazioni di risincronizzazione inversa sono le stesse di quelle sulla relazione di protezione originale.

Se non esistono policy e pianificazioni, vengono create.

Passi

1. Dalla pagina **Relazioni volume**, seleziona uno o più volumi con le relazioni che desideri invertire e, sulla barra degli strumenti, fai clic su **Inverti risincronizzazione**.

Viene visualizzata la finestra di dialogo Risincronizzazione inversa.

2. Verificare che le relazioni visualizzate nella finestra di dialogo **Risincronizzazione inversa** siano quelle per cui si desidera eseguire l'operazione di risincronizzazione inversa, quindi fare clic su **Invia**.

Viene avviata l'operazione di risincronizzazione inversa, si torna alla pagina Relazioni volume e nella parte superiore della pagina viene visualizzato un collegamento ai processi.

3. **Facoltativo:** fare clic su **Visualizza processi** nella pagina **Relazioni volume** per monitorare lo stato di ciascun processo di risincronizzazione inversa.

Viene visualizzato un elenco filtrato dei lavori correlati a questa operazione.

4. **Facoltativo:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni di volume**.

L'operazione di risincronizzazione inversa termina quando tutte le attività di lavoro vengono completate correttamente.

Ripristinare i dati utilizzando le pagine Volume e Dettagli volume/integrità

È possibile ripristinare file, directory o un intero volume sovrascritti o eliminati da una copia Snapshot utilizzando la funzionalità di ripristino nelle pagine Volume e Dettagli volume/integrità.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.



Si prega di notare i 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 ha una relazione intercluster e il cluster di destinazione non è ancora stato individuato.
 - Il volume è configurato per la replica sincrona SnapMirror .

Passi

1. Dal riquadro di navigazione a sinistra, vai a **Archiviazione > Volumi**.
2. Selezionare il volume e fare clic sul pulsante **Ripristina**. In alternativa, fare clic sul volume per andare a **Dettagli volume/integrità > Azioni > Ripristina**. Viene visualizzata la finestra di dialogo Ripristina. Per informazioni su questa pagina, vedere "[Finestra di dialogo 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 che si desidera ripristinare, ad esempio il LUN di origine.

È possibile ripristinare l'intero volume oppure specificare le cartelle e i file che si desidera ripristinare.

5. Selezionare la posizione in cui si desidera ripristinare gli elementi selezionati: **Posizione originale o Posizione alternativa esistente**.
6. Se selezioni una posizione alternativa esistente, esegui una delle seguenti operazioni:
 - Nel campo di testo Percorso di ripristino, digitare il percorso della posizione in cui si desidera ripristinare i dati, quindi fare clic su **Seleziona directory**.
 - Fare clic su **Sfoglia** per avviare la finestra di dialogo Sfoglia directory e completare i seguenti passaggi:
 - i. Selezionare il cluster di destinazione, la VM di archiviazione (SVM) e il volume su cui si desidera effettuare il ripristino.
 - ii. Nella tabella Nome, selezionare il nome della directory che si desidera ripristinare.
 - iii. Fare clic su **Seleziona directory**.
7. Fare clic su **Ripristina**.

Inizia il processo di ripristino. Per completare il processo di ripristino viene creato un processo nel backend.

8. Se si desidera visualizzare l'avanzamento del processo, dal riquadro di navigazione a sinistra, andare su **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 NetApp Console.

Quali sono i pool di risorse

I pool di risorse sono gruppi di aggregati creati da un amministratore di storage tramite Unified Manager per fornire il provisioning alle applicazioni partner per la gestione del backup.

È possibile raggruppare le risorse in base ad attributi quali prestazioni, costi, ubicazione fisica o disponibilità. Raggruppando le risorse correlate in un pool, è possibile trattare il pool come un'unica unità per il monitoraggio e il provisioning. Ciò semplifica la gestione di queste risorse e consente un utilizzo più flessibile ed efficiente dello storage.

Durante il provisioning dell'archiviazione secondaria, Unified Manager determina l'aggregato più adatto nel pool di risorse per la protezione utilizzando i seguenti criteri:

- L'aggregato è un aggregato di dati (non un aggregato radice) 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 ha lo spazio disponibile più grande tra tutti gli aggregati nel pool di risorse.
- Dopo aver effettuato il provisioning del volume di destinazione, lo spazio aggregato rientra nella soglia quasi piena e quasi sovraimpegnata definita per l'aggregato (soglia globale o locale, a seconda dei casi).
- Il numero di volumi FlexVol sul nodo di destinazione non deve superare il limite della piattaforma.

Creare pool di risorse

È possibile utilizzare la finestra di dialogo **Crea pool di risorse** per raggruppare gli aggregati a scopo di provisioning.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

I pool di risorse possono contenere aggregati provenienti da cluster diversi, ma lo stesso aggregato non può appartenere a un pool di risorse diversi.

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Pool di risorse**.
2. Nella pagina **Pool di risorse**, fare clic su **Crea**.
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 pool di risorse

È possibile modificare un pool di risorse esistente quando si desidera cambiarne il nome e la descrizione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Il pulsante **Modifica** è abilitato solo quando è selezionato un pool di risorse. Se viene selezionato più di un pool di risorse, il pulsante **Modifica** è disabilitato.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Pool di risorse**.
2. Selezionare un pool di risorse dall'elenco.
3. Fare clic su **Modifica**.

Viene visualizzata la finestra **Modifica pool di risorse**.

4. Modificare il nome e la descrizione del pool di risorse secondo necessità.
5. Fare clic su **Salva**.

Il nuovo nome e la nuova descrizione vengono visualizzati nell'elenco del pool di risorse.

Visualizza l'inventario dei pool di risorse

È possibile utilizzare la pagina Pool di risorse per visualizzare l'inventario dei pool di risorse e monitorare la capacità rimanente per ciascun pool di risorse.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Fare un passo

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Pool di risorse**.

Viene visualizzato l'inventario del pool di risorse.

Aggiungi membri al pool di risorse

Un pool di risorse è costituito da un certo numero di aggregati di membri. È possibile aggiungere aggregati ai pool di risorse esistenti per aumentare la quantità di spazio disponibile per il provisioning del volume secondario.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Non è possibile aggiungere più di 200 aggregati contemporaneamente a un pool di risorse. Gli aggregati mostrati nella finestra di dialogo Aggregati non appartengono ad alcun altro pool di risorse.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Pool di risorse**.
2. Selezionare un pool di risorse dall'elenco **Pool di risorse**.

I membri del pool di risorse vengono visualizzati nell'area sottostante l'elenco del pool di risorse.

3. Nell'area membri 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.

Rimuovere gli 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 un altro scopo.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

I membri del pool di risorse vengono visualizzati solo quando è selezionato un pool di risorse.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Pool di risorse**.
2. Selezionare il pool di risorse da cui si desidera rimuovere gli aggregati dei membri.

L'elenco degli aggregati dei membri viene visualizzato nel riquadro Membri.

3. Selezionare uno o più aggregati.

Il pulsante **Rimuovi** è abilitato.

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 riquadro Membri.

Elimina pool di risorse

È possibile eliminare i pool di risorse quando non sono più necessari. Ad esempio, potresti voler ridistribuire gli aggregati dei membri da un pool di risorse a diversi altri pool di risorse, rendendo obsoleto il pool di risorse originale.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Il pulsante **Elimina** è abilitato solo quando è selezionato almeno un pool di risorse.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Pool di risorse**.
2. Seleziona il pool di risorse che desideri eliminare.
3. Fare clic su **Elimina**.

Il pool di risorse viene rimosso dall'elenco dei pool di risorse e i suoi aggregati vengono rimossi dall'elenco dei membri.

Monitorare le relazioni di protezione del ripristino di emergenza della VM di archiviazione

Active IQ Unified Manager supporta il monitoraggio delle relazioni di disaster recovery delle VM di storage, garantendo il disaster recovery con la granularità del livello di una VM di storage. Il ripristino di emergenza della VM di archiviazione consente il ripristino dei dati presenti nei volumi costituenti della VM di archiviazione e il ripristino della configurazione della VM di archiviazione.

Viene creata una relazione DR della VM di archiviazione dalla VM di archiviazione di origine alla VM di archiviazione di destinazione per fornire un ripristino di emergenza asincrono. È possibile scegliere di replicare tutta o una parte della configurazione della VM di archiviazione (esclusa la configurazione di rete e protocollo) insieme ai volumi di dati in base alla configurazione del cluster.

Dopo aver configurato la relazione di disaster recovery della VM di archiviazione, quando la VM di archiviazione di origine non è più disponibile a causa di un guasto hardware o di un disastro ambientale, viene avviata la VM di archiviazione di destinazione, che fornisce l'accesso ai dati con la minima interruzione. Allo stesso modo, quando la VM di archiviazione di origine diventa disponibile, viene risincronizzata con la VM di archiviazione di destinazione e quindi la VM di origine si riavvia per fornire dati. È possibile utilizzare i comandi SnapMirror per configurare e gestire la relazione di disaster recovery della VM di archiviazione.

Monitora le VM di archiviazione utilizzando la pagina Relazioni

È possibile monitorare le relazioni di disaster recovery della VM di archiviazione dalla pagina Relazioni nella sezione PROTEZIONE dell'INVENTARIO. Per impostazione predefinita, la pagina Relazioni elenca solo le relazioni di livello superiore quando viene applicato il filtro delle relazioni costituenti.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile utilizzare i filtri per visualizzare le relazioni di disaster recovery delle VM di archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **PROTEZIONE > Relazioni**.

La pagina visualizza tutti i tipi di relazioni: relazioni tra volumi, gruppi di coerenza e VM di archiviazione.

2. Fare clic su **Filtro**, quindi selezionare **Tipo di oggetto relazione** e **VM di archiviazione** per visualizzare solo le relazioni di ripristino di emergenza della VM di archiviazione.
3. Fare clic su **Applica filtro**.



È necessario cancellare il filtro delle relazioni costituenti per visualizzare tutte le relazioni di protezione.

Nella pagina vengono visualizzate solo le relazioni di disaster recovery delle VM di archiviazione.

Visualizza le relazioni di protezione dalla pagina VM di archiviazione

Utilizzando la pagina VM di archiviazione, è possibile visualizzare lo stato delle relazioni di disaster recovery delle VM di archiviazione esistenti.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È inoltre possibile esaminare i dettagli delle relazioni di protezione, tra cui lo stato di trasferimento e ritardo, nonché i dettagli di origine e destinazione. È possibile pianificare report o scaricare report esistenti nel formato desiderato. Il pulsante **Mostra/Nascondi** consente di aggiungere le colonne richieste ai report, poiché non vengono visualizzate per impostazione predefinita.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **ARCHIVIAZIONE > VM di archiviazione**.
2. Dal menu **VISUALIZZA**, seleziona **Relazione > Tutte le relazioni**.

La vista Relazione: tutte le relazioni viene visualizzata con tutte le VM di archiviazione configurate.

Visualizza le VM di archiviazione in base allo stato di protezione

È possibile utilizzare la pagina VM di archiviazione dell'inventario per visualizzare tutte le VM di archiviazione in Active IQ Unified Manager e filtrare le VM di archiviazione in base al loro stato di protezione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Alla vista delle VM di archiviazione è stata aggiunta una nuova colonna Ruolo di protezione che fornisce informazioni sul fatto che la VM di archiviazione sia protetta o meno.



Se un cluster di origine non viene aggiunto ad Active IQ Unified Manager, tutte le informazioni relative a tale cluster non saranno disponibili nelle griglie.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **ARCHIVIAZIONE > VM di archiviazione**.
2. Dal menu **VISUALIZZA**, seleziona **Integrità > Tutte le VM di archiviazione**.

Viene visualizzata la schermata Integrità: tutte le VM di archiviazione.

3. Fare clic su **Filtro** per visualizzare una delle seguenti VM di archiviazione.

Per visualizzare	Valore del filtro
VM con archiviazione protetta	Ruolo di protezione è Protetto
VM di archiviazione non protette	Il ruolo di protezione è non protetto



Non è possibile visualizzare contemporaneamente sia le VM di archiviazione protette che quelle non protette. Sarà necessario cancellare il filtro esistente per riapplicare una nuova opzione di filtro.

4. Fare clic su **Applica filtro**.

La vista Non salvate mostra tutte le VM di archiviazione protette o non protette dal ripristino di emergenza delle VM di archiviazione in base alle selezioni dei filtri.

Informazioni sulle associazioni delle VM di archiviazione

Le associazioni di macchine virtuali di archiviazione (VM di archiviazione) sono mappature da una VM di archiviazione di origine a una VM di archiviazione di destinazione, utilizzate dalle applicazioni partner per la selezione delle risorse e il provisioning dei volumi secondari.

Le associazioni vengono create tra una VM di archiviazione di origine e una VM di archiviazione di destinazione, indipendentemente dal fatto che la VM di archiviazione di destinazione sia una destinazione secondaria o terziaria. Non è possibile utilizzare una VM di archiviazione di destinazione secondaria come origine per creare un'associazione con una VM di archiviazione di destinazione terziaria.

In qualità di amministratore dell'applicazione o amministratore dell'archiviazione, puoi visualizzare le associazioni delle VM di archiviazione nel tuo ambiente nella pagina **Protezione > Associazioni VM di archiviazione**.

È possibile associare le SVM in tre modi:

- **Associa qualsiasi VM di archiviazione:** puoi creare un'associazione tra qualsiasi VM di archiviazione di origine primaria e una o più SVM di destinazione. Ciò significa che tutte le SVM esistenti che attualmente necessitano di protezione, nonché tutte le SVM che verranno create in futuro, sono associate alle SVM di destinazione specificate. Ad esempio, potresti voler eseguire il backup di applicazioni provenienti da diverse origini in posizioni diverse su una o più SVM di destinazione in un'unica posizione.
- **Associa una VM di archiviazione specifica:** puoi creare un'associazione tra una VM di archiviazione di origine specifica e una o più SVM di destinazione specifiche. Ad esempio, se si forniscono servizi di archiviazione a molti client i cui dati devono essere separati l'uno dall'altro, è possibile scegliere questa opzione per associare una specifica VM di archiviazione di origine a una specifica VM di archiviazione di destinazione assegnata solo a quel client.
- **Associa a una VM di archiviazione esterna:** puoi creare un'associazione tra una VM di archiviazione di origine e un volume flessibile esterno di una VM di archiviazione di destinazione.

Creare associazioni di VM di archiviazione

La procedura guidata Crea associazioni di macchine virtuali di archiviazione consente alle applicazioni di protezione dei partner di associare una VM di archiviazione di origine a una VM di archiviazione di destinazione per l'utilizzo con relazioni SnapMirror e SnapVault. Le applicazioni partner utilizzano queste associazioni al momento del provisioning iniziale dei volumi di destinazione per determinare quali risorse selezionare.dd

Prima di iniziare

- La VM di archiviazione che stai associando deve già esistere.
- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per qualsiasi VM di archiviazione di origine e tipo di relazione, è possibile scegliere una sola VM di archiviazione di destinazione su ciascun cluster di destinazione.

La modifica delle associazioni tramite le funzioni di eliminazione e creazione influisce solo sulle future operazioni di provisioning. Non sposta i volumi di destinazione esistenti.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Associazioni VM di archiviazione**.
2. Nella pagina **Associazioni VM di archiviazione**, fare clic su **Crea**.

Viene avviata la procedura guidata **Crea associazioni macchine virtuali di archiviazione**.

3. Seleziona una delle seguenti fonti:

- **Qualunque**

Selezionare questa opzione quando si desidera creare un'associazione tra una qualsiasi VM di archiviazione primaria di origine e una o più VM di archiviazione di destinazione. Ciò significa che tutte le VM di archiviazione esistenti che attualmente necessitano di protezione, nonché tutte le VM di archiviazione che verranno create in futuro, sono associate alla VM di archiviazione di destinazione specificata. Ad esempio, potresti voler eseguire il backup di applicazioni provenienti da diverse origini in posizioni diverse su una o più VM di archiviazione di destinazione in un'unica posizione.

- **Separare**

Selezionare questa opzione quando si desidera selezionare una specifica VM di archiviazione di origine associata a una o più VM di archiviazione di destinazione. Ad esempio, se si forniscono servizi di archiviazione a molti client i cui dati devono essere separati l'uno dall'altro, scegliere questa opzione per associare una specifica origine VM di archiviazione a una specifica destinazione VM di archiviazione assegnata solo a quel client.

- **Nessuno (esterno)**

Selezionare questa opzione quando si desidera creare un'associazione tra una VM di archiviazione di origine e un volume flessibile esterno di una VM di archiviazione di destinazione.

4. Seleziona uno o entrambi i tipi di relazione di protezione che desideri creare:

- * SnapMirror*
- * SnapVault*

5. Fare clic su **Avanti**.

6. Selezionare una o più destinazioni di protezione delle VM di archiviazione.

7. Fare clic su **Fine**.

Elimina le associazioni delle VM di archiviazione

È possibile eliminare le associazioni delle VM di archiviazione per le applicazioni partner per rimuovere la relazione di provisioning secondaria tra la VM di archiviazione di origine e quella di destinazione; ad esempio, è possibile eseguire questa operazione quando la VM di archiviazione di destinazione è piena e si desidera creare nuove associazioni di protezione per la VM di archiviazione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Il pulsante **Elimina** è disabilitato finché non viene selezionata almeno un'associazione VM di archiviazione. La modifica delle associazioni tramite le funzioni di eliminazione e creazione influisce solo sulle future operazioni di provisioning; non sposta i volumi di destinazione esistenti.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Associazioni VM di archiviazione**.
2. Selezionare almeno un'associazione VM di archiviazione.

Il pulsante **Elimina** è abilitato.

3. Fai clic su **Elimina**.

Viene visualizzata una finestra di dialogo di avviso.

4. Fare clic su **Sì** per continuare.

L'associazione VM di archiviazione selezionata viene rimossa dall'elenco.

Requisiti SVM e pool di risorse per supportare i servizi di archiviazione

È possibile garantire meglio la conformità nelle applicazioni partner se si osservano

alcuni requisiti di associazione SVM e pool di risorse specifici dei servizi di archiviazione: 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 archiviazione 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 posizioni secondarie o terziarie. Per supportare questi servizi di archiviazione della 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 archiviazione, inclusa la replica da un volume di origine SnapMirror o primario SnapVault a SnapMirror di destinazione o a volumi di backup SnapVault che risiedono in posizioni secondarie o terziarie, osservare i seguenti requisiti:

- Le associazioni SVM devono essere configurate tra l'SVM contenente il volume sorgente SnapMirror o il volume primario SnapVault e qualsiasi SVM su cui risiede un volume secondario o un volume terziario.
 - Ad esempio, per supportare una topologia di protezione in cui il volume di origine Vol_A risiede su SVM_1, il volume di destinazione secondario SnapMirror Vol_B risiede su SVM_2 e il volume di backup terziario SnapVault 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 SnapMirror o associazione di backup SnapVault tra SVM_2 e SVM_3 non è necessaria e non viene utilizzata.

- Per supportare una topologia di protezione in cui sia il volume di origine Vol_A sia 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 risorse aggregate del cluster disponibili per le SVM associate.

È possibile configurare i pool di risorse tramite l'interfaccia utente Web di Unified Manager e quindi assegnare tramite l'applicazione partner i nodi di destinazione secondaria e terziaria del servizio di archiviazione.

Quali sono i lavori

Un lavoro è una serie di attività che è possibile monitorare tramite Unified Manager. Visualizzando i lavori e le attività associate è possibile stabilire se sono stati completati correttamente.

I processi vengono avviati quando si creano relazioni SnapMirror e SnapVault, quando si esegue un'operazione di relazione (interruzione, modifica, disattivazione, rimozione, ripresa, risincronizzazione e risincronizzazione inversa), 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.

Monitorare i lavori

È possibile utilizzare la pagina Lavori per monitorare lo stato dei lavori e visualizzare le

proprietà dei lavori, ad esempio il tipo di servizio di archiviazione, lo stato, l'ora di invio e l'ora di completamento, per determinare se un lavoro è stato completato correttamente o meno.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Lavori**.

Viene visualizzata la pagina Lavori.

2. Visualizza la colonna **Stato** per determinare lo stato dei processi attualmente in esecuzione.
3. Fare clic sul nome di un lavoro per visualizzarne i dettagli.

Viene visualizzata la pagina dei dettagli del lavoro.

Visualizza i dettagli del lavoro

Dopo aver avviato un lavoro, puoi seguirne l'avanzamento dalla pagina dei dettagli del lavoro e monitorare le attività associate per individuare eventuali errori.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a 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 informazioni aggiuntive nel riquadro **Dettagli attività** e nel riquadro **Messaggi attività** a destra dell'elenco attività.

Interrompere i lavori

È possibile utilizzare la pagina Lavori per annullare un lavoro se impiega troppo tempo per essere completato, riscontra troppi errori o non è più necessario. È possibile annullare un processo solo se il suo stato e il suo tipo lo consentono. È possibile interrompere qualsiasi processo in esecuzione.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Lavori**.
2. Dall'elenco dei lavori, selezionarne uno, quindi fare clic su **Interrompi**.
3. Alla richiesta di conferma, fare clic su **Sì** per annullare il processo selezionato.

Riprova un processo di protezione non riuscito

Dopo aver adottato misure per risolvere un processo di protezione non riuscito, è possibile utilizzare **Riprova** per eseguire nuovamente il processo. Riprovando un processo, viene creato un nuovo processo utilizzando l'ID processo originale.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile riprovare solo un lavoro non riuscito alla volta. Selezionando più di un lavoro il pulsante **Riprova** viene disattivato. È possibile ripetere l'operazione solo per i processi di tipo Configurazione di protezione e Operazione di relazione di protezione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Protezione > Lavori**.
2. Dall'elenco dei processi, selezionare un singolo processo di tipo Configurazione di protezione o Operazione di relazione di protezione non riuscito.

Il pulsante **Riprova** è abilitato.

3. Fare clic su **Riprova**.

Il lavoro viene riavviato.

Descrizione delle finestre e delle finestre di dialogo delle relazioni di protezione

È possibile visualizzare e gestire i dettagli relativi alla protezione, quali 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 Pool di risorse

La pagina Pool di risorse visualizza i pool di risorse esistenti e i relativi membri e consente di creare, monitorare e gestire i pool di risorse per scopi di provisioning.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Creare**

Avvia la finestra di dialogo Crea pool di risorse, che puoi utilizzare per creare pool di risorse.

- **Modificare**

Consente di modificare il nome e la descrizione dei pool di risorse creati.

- **Eliminare**

Consente di eliminare uno o più pool di risorse.

Elenco dei pool di risorse

L'elenco Pool di risorse visualizza (in formato tabellare) 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 SnapLock sono Conformità, Azienda e Non- SnapLock. Un pool di risorse può contenere aggregati di un solo tipo 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.

- **Usato %**

Visualizza la percentuale di spazio utilizzato nel pool di risorse.

Pulsanti di comando dell'elenco dei membri

I pulsanti di comando dell'elenco Membri consentono di eseguire le seguenti attività:

- **Aggiungere**

Consente di aggiungere membri al pool di risorse.

- **Eliminare**

Consente di eliminare uno o più membri dal pool di risorse.

Elenco dei membri

L'elenco Membri visualizza (in formato tabellare) i membri del pool di risorse e le relative proprietà quando viene selezionato un pool di risorse.

- **Stato**

Visualizza lo stato attuale dell'aggregato dei membri. Lo stato può essere Critico (❌), Errore (💡), Avvertimento (⚠️), o Normale (✅).

- **Nome aggregato**

Visualizza il nome dell'aggregato dei membri.

- **Stato**

Visualizza lo stato corrente dell'aggregato, che può essere uno dei seguenti:

- Fuori linea

L'accesso in lettura o scrittura non è consentito.

- In linea

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

L'aggregato è in fase di creazione.

- Distruggendo

L'aggregato viene distrutto.

- Fallito

L'aggregato non può essere messo online.

- Congelato

L'aggregato (temporaneamente) non sta elaborando le richieste.

- Incoerente

L'aggregato è stato contrassegnato come danneggiato; contattare l'assistenza tecnica.

- Ferro limitato

Gli strumenti diagnostici non possono essere eseguiti in modo aggregato.

- Montaggio

L'aggregato è in fase di montaggio.

- Parziale

È stato trovato almeno un disco per l'aggregato, ma ne mancano due o più.

- Quiescenza

L'aggregato è in fase di sospensione.

- Quieced

L'aggregato è inattivo.

- Ripristinato

Il ripristino di un aggregato è completato.

- Smontato

L'aggregato è stato smontato.

- Smontaggio

L'aggregato verrà disattivato.

- Sconosciuto

L'aggregato è stato rilevato, ma le informazioni aggregate non sono ancora state recuperate dal server Unified Manager.

Per impostazione predefinita, questa colonna è nascosta.

- **Grappolo**

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 in totale.

- **Usato %**

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 e descrivere un nuovo pool di risorse e per aggiungere ed eliminare aggregati da tale pool di risorse.

Nome del pool di risorse

Le caselle di testo consentono di aggiungere le seguenti informazioni per creare un pool di risorse:

Consente di specificare un nome per il 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 attività:

- **Aggiungere**

Apri la finestra di dialogo Aggregati in modo da poter 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.

- **Rimuovere**

Consente di rimuovere gli aggregati selezionati dal pool di risorse.

- **Creare**

Crea il pool di risorse. Questo pulsante non è abilitato finché non vengono inserite informazioni nei campi Nome pool di risorse o Descrizione.

- **Cancellare**

Annulla le modifiche e chiude la finestra di dialogo Crea pool di risorse.

Finestra di dialogo Modifica pool di risorse

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 errati, puoi modificarli per renderli più precisi.

Caselle di testo

Le caselle di testo consentono di modificare le seguenti informazioni per il pool di risorse selezionato:

- **Nome del pool di risorse**

Consente di immettere un nuovo nome.

- **Descrizione**

Consente di immettere una nuova descrizione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Salva**

Salva le modifiche apportate al nome e alla descrizione del pool di risorse.

- **Cancellare**

Annulla 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 attività:

- **Aggiungere**

Aggiunge gli aggregati selezionati al pool di risorse. Il pulsante Aggiungi non è abilitato finché non viene selezionato almeno un aggregato.

- **Cancellare**

Annulla le modifiche e chiude la finestra di dialogo Aggregati.

Elenco degli aggregati

L'elenco Aggregati visualizza (in formato tabellare) i nomi e le proprietà degli aggregati monitorati.

- **Stato**

Visualizza lo stato corrente di un volume. Lo stato può essere Critico (❌), Errore (⚠️), Avvertimento (⚠️), o Normale (✅).

È possibile spostare il puntatore sullo stato per visualizzare maggiori 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:

- Fuori linea

L'accesso in lettura o scrittura non è consentito.

- Limitato

Sono consentite operazioni limitate (come la ricostruzione della parità), ma non è consentito l'accesso ai dati.

- In linea

È consentito l'accesso in lettura e scrittura ai volumi ospitati su questo aggregato.

- Creazione

L'aggregato è in fase di creazione.

- Distruggendo

L'aggregato viene distrutto.

- Fallito

L'aggregato non può essere messo online.

- Congelato

L'aggregato (temporaneamente) non sta elaborando le richieste.

- Incoerente

L'aggregato è stato contrassegnato come danneggiato; contattare l'assistenza tecnica.

- Ferro limitato

Gli strumenti diagnostici non possono essere eseguiti in modo aggregato.

- Montaggio

L'aggregato è in fase di montaggio.

- Parziale

È stato trovato almeno un disco per l'aggregato, ma ne mancano due o più.

- Quiescenza

L'aggregato è in fase di sospensione.

- Quieced

L'aggregato è inattivo.

- Ripristinato

Il ripristino di un aggregato è completato.

- Smontato

L'aggregato è offline.

- Smontaggio

L'aggregato verrà disattivato.

- Sconosciuto

L'aggregato è stato rilevato, ma le informazioni aggregate non sono ancora state recuperate dal server Unified Manager.

- **Grappolo**

Visualizza il nome del cluster su cui risiede l'aggregato.

- **Nodo**

Visualizza il nome del controller di archiviazione che contiene l'aggregato.

- **Capacità totale**

Visualizza la dimensione totale 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 aggregati. Per impostazione predefinita, questa colonna è nascosta.

- **Disponibile %**

Visualizza la percentuale di spazio disponibile per i dati aggregati. Per impostazione predefinita, questa colonna è nascosta.

- **Usato %**

Visualizza la percentuale di spazio utilizzata dai dati nell'aggregato.

- **Tipo RAID**

Visualizza il tipo RAID del volume selezionato. Il tipo di RAID può essere RAID0, RAID4, RAID-DP, RAID-TEC o RAID misto.

Pagina dei lavori

La pagina Lavori consente di visualizzare lo stato corrente e altre informazioni su tutti i lavori di protezione delle applicazioni partner attualmente in esecuzione, nonché sui lavori completati. È possibile utilizzare queste informazioni per vedere quali processi sono ancora in esecuzione e se un processo è riuscito o meno.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Interrompi**

Interrompe il lavoro selezionato. Questa opzione è disponibile solo se il lavoro selezionato è in esecuzione.

- **Riprova**

Riavvia un processo non riuscito di tipo Configurazione di protezione o Operazione di relazione di protezione. È possibile riprovare solo un lavoro non riuscito alla volta. Se viene selezionato più di un processo non riuscito, il pulsante **Riprova** è disabilitato. Non è possibile riprovare i processi del servizio di archiviazione non riusciti.

- **Aggiorna**

Aggiorna l'elenco dei lavori e le informazioni ad essi associate.

Elenco dei lavori

L'elenco Lavori visualizza, in formato tabellare, 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 Errore () 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 quando avvia il lavoro. È possibile cercare un lavoro specifico inserendo il numero di identificazione del lavoro nella casella di testo fornita dal filtro della colonna.

- **Nome**

Visualizza il nome del lavoro.

- **Tipo**

Visualizza il tipo di lavoro. Le tipologie di lavoro sono le seguenti:

- **Acquisizione di cluster**

Un processo di automazione del flusso di lavoro sta riscoprendo un cluster.

- **Configurazione di protezione**

Un processo di protezione avvia flussi di lavoro di automazione del flusso di lavoro, come pianificazioni cron, creazione di policy SnapMirror e così via.

- **Operazione di relazione di protezione**

Un processo di protezione sta eseguendo operazioni SnapMirror .

- **Catena del flusso di lavoro di protezione**

Un processo di automazione del flusso di lavoro esegue più flussi di lavoro.

- **Ripristinare**

È in esecuzione un processo di ripristino.

- **Ripulire**

Il lavoro consiste nel ripulire gli artefatti dei membri del servizio di archiviazione che non sono più necessari per scopi di ripristino.

- **Conformarsi**

Il lavoro consiste nel controllare la configurazione dei membri del servizio di archiviazione per garantirne la conformità.

- **Distruggere**

Il lavoro sta distruggendo un servizio di archiviazione.

- **Importare**

Il lavoro consiste nell'importare oggetti di archiviazione non gestiti in un servizio di archiviazione esistente.

- **Modificare**

Il lavoro consiste nel modificare gli attributi di un servizio di archiviazione esistente.

- **Iscriviti**

Il lavoro consiste nell'iscrivere i membri a un servizio di archiviazione.

- **Annulla iscrizione**

Il lavoro consiste nell'annullare l'iscrizione dei membri a un servizio di archiviazione.

- **Aggiornamento**

È in esecuzione un processo di aggiornamento della protezione.

- **Configurazione WFA**

Un processo di automazione del flusso di lavoro sta inviando 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:

- **Abortito**

Il lavoro è stato interrotto.

- **Interruzione**

Il lavoro è in fase di interruzione.

- **Completato**

Il lavoro è terminato.

- **Corsa**

Il lavoro è in esecuzione.

- **Ora di invio**

Visualizza l'ora in cui il lavoro è stato inviato.

- **Durata**

Visualizza il tempo impiegato per completare il lavoro. Questa colonna è visualizzata per impostazione predefinita.

- **Ora completata**

Visualizza l'ora in cui il lavoro è terminato. Per impostazione predefinita, questa colonna è nascosta.

Pagina dei dettagli del lavoro

La pagina Dettagli processo 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 l'avanzamento dei processi di protezione e per risolvere i problemi relativi ai processi non riusciti.

Riepilogo del lavoro

Il riepilogo del lavoro mostra le seguenti informazioni:

- ID lavoro

- Tipo
- Stato
- Ora di invio
- Tempo di completamento
- Durata

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Aggiorna**

Aggiorna l'elenco delle attività e le proprietà associate a ciascuna attività.

- **Visualizza lavori**

Ti riporta alla pagina Lavori.

Elenco delle attività lavorative

L'elenco delle attività di lavoro visualizza in una tabella tutte le attività associate a un lavoro specifico e le proprietà relative 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, mentre quelle più vecchie vengono visualizzate nella parte inferiore.

- **Tipo**

Visualizza il tipo di attività.

- **Stato**

Lo stato di un compito particolare:

- **Completato**

Il compito è terminato.

- **In coda**

L'attività sta per essere eseguita.

- **Corsa**

L'attività è in esecuzione.

- **In attesa**

È stato inviato un lavoro e alcune attività associate sono in attesa di essere messe in coda ed eseguite.

- **Stato**

Visualizza lo stato dell'attività:

- **Errore** ()

Il compito è fallito.

- **Normale** ()

Il compito è riuscito.

- **Saltato** ()

Un'attività non è riuscita e le attività successive sono state saltate.

- **Durata**

Visualizza il tempo trascorso dall'inizio dell'attività.

- **Ora completata**

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 delle attività in un grafico, assegnando zero alla prima attività. Per impostazione predefinita, questa colonna è nascosta.

- **Riquadro Dettagli attività**

Visualizza informazioni aggiuntive su ogni attività lavorativa, tra cui il nome dell'attività, la descrizione dell'attività e, se l'attività non è riuscita, il motivo dell'errore.

- **Riquadro Messaggi attività**

Visualizza messaggi specifici per l'attività selezionata. I messaggi potrebbero includere il motivo dell'errore e suggerimenti per risolverlo. Non tutte le attività visualizzano messaggi di attività.

Finestra di dialogo Impostazioni secondarie avanzate

È possibile utilizzare la finestra di dialogo Impostazioni secondarie avanzate per abilitare la replica flessibile in base alla versione, il backup di più copie e le impostazioni relative allo spazio su un volume secondario. È possibile utilizzare la finestra di dialogo Impostazioni secondarie avanzate quando si desidera modificare, abilitare o disabilitare le impostazioni correnti.

Le impostazioni relative allo spazio massimizzano la quantità di dati archiviati, tra cui: deduplicazione, compressione dei dati, aumento automatico e garanzia dello spazio.

La finestra di dialogo include i seguenti campi:

- **Abilita replica flessibile in base alla versione**

Abilita SnapMirror con replica flessibile in base alla versione. La replica flessibile in base alla versione consente la protezione SnapMirror di un volume di origine anche se il volume di destinazione è in esecuzione con una versione di ONTAP precedente a quella del volume di origine.

- Abilita backup

Se è abilitata la replica flessibile in base alla versione, consente anche il trasferimento e la conservazione di più copie Snapshot dei dati di origine SnapMirror nella destinazione SnapMirror .

- **Abilita deduplicazione**

Abilita la deduplicazione sul volume secondario in una relazione SnapVault in modo da eliminare i blocchi di dati duplicati e ottenere un risparmio di spazio. È possibile utilizzare la deduplicazione quando il risparmio di spazio è pari ad almeno il 10 per cento e quando la velocità di sovrascrittura dei dati non è elevata. La deduplicazione viene spesso utilizzata per ambienti virtualizzati, condivisioni di file e dati di backup. Questa impostazione è disabilitata per impostazione predefinita. Se abilitata, questa operazione viene avviata dopo ogni trasferimento.

- Abilita compressione

Abilita la compressione trasparente dei dati. È possibile utilizzare la compressione quando il risparmio di spazio è pari ad almeno il 10 per cento, quando il potenziale sovraccarico 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 disabilitata per impostazione predefinita. La compressione è disponibile solo quando è selezionata la deduplicazione.

- Comprimi in linea

Consente un risparmio immediato di spazio comprimendo i dati prima di scriverli sul disco. È possibile utilizzare la compressione in linea quando il sistema non è utilizzato più del 50 per cento durante le ore di punta e quando il sistema può gestire nuove scritture e CPU aggiuntiva durante le ore di punta. Questa impostazione è disponibile solo quando è selezionata l'opzione "Abilita compressione".

- **Abilita crescita automatica**

Consente di aumentare automaticamente il volume di destinazione quando la percentuale di spazio libero è inferiore alla soglia specificata, a condizione che ci sia spazio disponibile sull'aggregato associato.

- **Dimensione massima**

Imposta la percentuale massima di crescita di un volume. L'impostazione predefinita è il 20 per cento maggiore della dimensione del volume di origine. Un volume non aumenta automaticamente se la dimensione corrente è maggiore o uguale alla percentuale massima di aumento automatico. Questo campo è abilitato solo quando è abilitata l'impostazione di aumento automatico.

- **Incremento dimensione**

Specifica l'incremento percentuale con cui il volume aumenta automaticamente prima di raggiungere la percentuale massima del volume sorgente.

- **Garanzia di spazio**

Garantisce che sul volume secondario sia allocato spazio sufficiente affinché i trasferimenti di dati vadano sempre a buon fine. L'impostazione della garanzia dello spazio può essere una delle seguenti:

- File
- Volume
- Nessuno + Ad esempio, potresti avere un volume da 200 GB che contiene 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 del volume di origine. La garanzia dei file alloca 50 GB per garantire che venga riservato spazio sufficiente per i file nell'origine; selezionando Nessuno in questo scenario, sulla destinazione vengono allocati solo 10 GB per lo spazio effettivamente utilizzato dai dati dei file nell'origine.

Per impostazione predefinita, la garanzia dello spazio è impostata su Volume.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Fare domanda a**

Salva le impostazioni di efficienza selezionate e le applica quando si fa clic su **Applica** nella finestra di dialogo Configura protezione.

- **Cancellare**

Annulla le selezioni e chiude la finestra di dialogo Impostazioni avanzate destinazione.

Finestra di dialogo Impostazioni di destinazione avanzate

È possibile utilizzare la finestra di dialogo Impostazioni di destinazione avanzate per abilitare le impostazioni di garanzia dello spazio su un volume di destinazione. È possibile selezionare impostazioni avanzate quando la garanzia dello spazio è disabilitata sull'origine, ma si desidera che sia abilitata sulla destinazione. Le impostazioni per la deduplicazione, la compressione e l'aumento automatico 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 affinché i trasferimenti di dati vadano sempre a buon fine. L'impostazione della garanzia dello spazio può essere una delle seguenti:

- File
- Volume
- Nessuno

Ad esempio, potresti avere un volume da 200 GB che contiene 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 del volume di origine. La garanzia dei file alloca 50 GB per garantire che venga riservato spazio sufficiente per i file di origine nella destinazione; selezionando **Nessuno** in questo scenario, sulla destinazione vengono allocati solo 10 GB per lo spazio effettivamente utilizzato dai dati dei file nell'origine.

Per impostazione predefinita, la garanzia dello spazio è impostata su Volume.

Finestra di dialogo Ripristina

È possibile utilizzare la finestra di dialogo Ripristina per ripristinare i dati su un volume da una copia Snapshot specifica.

Ripristina da

L'area Ripristina da consente di specificare da dove si desidera ripristinare i dati.

- **Volume**

Specifica il volume da cui 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 che contiene tutti i volumi con relazioni di protezione con il volume su cui è stata avviata l'azione di ripristino.

- **Copia istantanea**

Specifica quale copia Snapshot si desidera utilizzare per ripristinare i dati. Per impostazione predefinita, viene selezionata la copia Snapshot più recente. È anche possibile selezionare una copia Snapshot diversa dall'elenco a discesa. L'elenco delle copie Snapshot cambia in base al volume selezionato.

- **Elenca un massimo di 995 file e directory**

Per impostazione predefinita, nell'elenco vengono visualizzati al massimo 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.

Seleziona gli elementi da ripristinare

L'area Seleziona elementi da ripristinare consente di selezionare l'intero volume o file e cartelle specifici che si desidera ripristinare. È possibile selezionare un massimo di 10 file, cartelle o una combinazione di entrambi. Quando è selezionato il numero massimo di elementi, le caselle di controllo per la selezione degli elementi sono disabilitate.

- **Campo percorso**

Visualizza il percorso dei dati che si desidera ripristinare. Puoi andare alla cartella e ai file che vuoi ripristinare oppure digitare il percorso. Questo campo è vuoto finché non selezioni o digiti un percorso.

Cliccando  dopo aver scelto un percorso si sale di un livello nella struttura delle directory.

- **Elenco cartelle e file**

Visualizza il contenuto del percorso immesso. Per impostazione predefinita, inizialmente viene visualizzata la cartella radice. Facendo clic sul nome di una cartella viene visualizzato il contenuto della cartella.

È possibile selezionare gli elementi da ripristinare come segue:

- Quando si immette il percorso con un nome file specifico specificato nel campo percorso, il file specificato viene visualizzato nelle cartelle e nei file.
- Quando si immette un percorso senza specificare un file specifico, 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 ci sono troppi elementi da visualizzare e, se si procede con l'operazione, tutti gli elementi nella cartella specificata verranno ripristinati. È possibile deselezionare la casella di controllo "Elenca massimo 995 file e directory" se si desidera visualizzare tutti gli oggetti all'interno del volume selezionato.



Non è possibile ripristinare i flussi di file NTFS.

Ripristinare a

L'area Ripristina in consente di specificare dove si desidera ripristinare i dati.

- **Posizione originale in Volume_Name**

Ripristina i dati selezionati nella directory di origine da cui è stato eseguito il backup dei dati.

- **Posizione alternativa**

Ripristina i dati selezionati in una nuova posizione:

- Ripristina percorso

Specifica un percorso alternativo per il ripristino dei dati selezionati. Il percorso deve già esistere. È possibile utilizzare il pulsante **Sfoglia** per passare alla posizione in cui si desidera ripristinare i dati oppure immettere manualmente il percorso utilizzando il formato cluster://svm/volume/path.

- Preserva la gerarchia delle directory

Se selezionata, questa opzione conserva 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 attività:

- **Cancellare**

Annulla le selezioni e chiude la finestra di dialogo Ripristina.

- **Ripristinare**

Applica le selezioni e avvia il processo di ripristino.

Finestra di dialogo Sfoglia directory

È possibile utilizzare la finestra di dialogo Sfoglia directory quando si desidera ripristinare i dati in una directory su un cluster e SVM diversa dalla sorgente originale. Per impostazione predefinita vengono selezionati il cluster e il volume di origine originali.

La finestra di dialogo Sfoglia directory consente di selezionare il cluster, l'SVM, il volume e il percorso della

directory in cui si desidera ripristinare i dati.

- **Grappolo**

Elenca le destinazioni cluster disponibili su cui è possibile effettuare il ripristino. Per impostazione predefinita, viene selezionato il cluster del volume sorgente originale.

- **Elenco a discesa SVM**

Elenca gli SVM disponibili per il cluster selezionato. Per impostazione predefinita, viene selezionato l'SVM del volume sorgente 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 sorgente originale.

- **Casella di testo del percorso del file**

Consente di digitare il percorso del file in cui si desidera ripristinare i dati. Il percorso inserito deve già esistere.

- **Nome**

Visualizza i nomi delle cartelle disponibili per il volume selezionato. Facendo clic su una cartella nell'elenco Nome vengono visualizzate le sottocartelle, se presenti. I file contenuti nelle cartelle non vengono visualizzati. Cliccando  dopo aver selezionato una cartella si sale di un livello nella struttura delle directory.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Seleziona directory**

Applica le selezioni e chiude la finestra di dialogo Sfoglia directory. Se non è selezionata alcuna directory, questo pulsante è disabilitato.

- **Cancellare**

Annulla le selezioni e chiude la finestra di dialogo Sfoglia directory.

Finestra di dialogo Configura protezione

È possibile utilizzare la finestra di dialogo Configura protezione per creare relazioni SnapMirror e SnapVault per tutti i volumi di lettura, scrittura e protezione dati sui cluster, per garantire che i dati su un volume di origine o primario vengano replicati.

Scheda Sorgente

- **Vista topologica**

Visualizza una rappresentazione visiva della relazione che stai creando. Per impostazione predefinita, la

sorgente nella topologia è evidenziata.

- **Informazioni sulla fonte**

Visualizza i dettagli sui volumi sorgente selezionati, comprese le seguenti informazioni:

- Nome del cluster di origine
- Nome SVM di origine
- Dimensione totale del volume cumulativo

Visualizza la dimensione totale di tutti i volumi sorgente selezionati.

- Dimensione del volume cumulativo utilizzato

Visualizza la dimensione cumulativa del volume utilizzato per tutti i volumi sorgente selezionati.

- Volume sorgente

Visualizza le seguenti informazioni in una tabella:

- Volume sorgente

Visualizza i nomi dei volumi sorgente selezionati.

- Tipo

Visualizza il tipo di volume.

- Tipo SnapLock

Visualizza il tipo di SnapLock del volume. Le opzioni sono Conformità, Azienda e Non- SnapLock.

- Copia istantanea

Visualizza la copia Snapshot utilizzata per il trasferimento della linea di base. Se il volume di origine è di lettura/scrittura, il valore Predefinito nella colonna Copia snapshot indica che per impostazione predefinita viene creata una nuova copia snapshot, che viene utilizzata per il trasferimento di base. Se il volume di origine è un volume di protezione dati, il valore Predefinito nella colonna Copia snapshot indica che non viene creata alcuna nuova copia snapshot e tutte le copie snapshot esistenti vengono trasferite alla destinazione. Facendo clic sul valore Copia snapshot viene visualizzato un elenco di copie snapshot da cui è possibile selezionare una copia snapshot esistente da utilizzare per il trasferimento di base. Non è possibile selezionare una copia Snapshot predefinita diversa se il tipo di origine è la protezione dei dati.

Scheda SnapMirror

Consente di specificare un cluster di destinazione, una macchina virtuale di archiviazione (SVM) e un aggregato per una relazione di protezione, nonché una convenzione di denominazione per le destinazioni durante la creazione di una relazione SnapMirror . È anche possibile specificare una politica e una pianificazione SnapMirror .

- **Vista topologica**

Visualizza una rappresentazione visiva della relazione che stai creando. Per impostazione predefinita, la risorsa di destinazione SnapMirror nella topologia è evidenziata.

• Informazioni sulla destinazione

Consente di selezionare le risorse di destinazione per una relazione di protezione:

- Collegamento avanzato

Avvia la finestra di dialogo Impostazioni di destinazione avanzate quando si crea una relazione SnapMirror .

- Grappolo

Elenca i cluster disponibili come host di destinazione della protezione. Questo campo è obbligatorio.

- macchina virtuale di archiviazione (SVM)

Elenca le SVM disponibili sul cluster selezionato. È necessario selezionare un cluster prima che l'elenco SVM venga popolato. Questo campo è obbligatorio.

- Aggregato

Elenca gli aggregati disponibili sull'SVM selezionato. È necessario selezionare un cluster prima che l'elenco Aggregato venga compilato. Questo campo è obbligatorio. L'elenco Aggregato visualizza le seguenti informazioni:

- Rango

Quando più aggregati soddisfano tutti i requisiti per una destinazione, il rango indica la priorità in cui l'aggregato è elencato, in base alle seguenti condizioni:

- A. Per consentire la separazione del dominio di errore, è preferibile un aggregato posizionato su un nodo diverso da quello del volume sorgente.
- B. È preferibile un aggregato su un nodo con meno volumi per consentire il bilanciamento del carico tra i nodi di un cluster.
- C. Per consentire il bilanciamento della capacità, è preferibile un aggregato che abbia più spazio libero rispetto ad altri aggregati. Un grado pari a 1 significa 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 denominazione

Specifica la convenzione di denominazione predefinita applicata al volume di destinazione. È possibile accettare la convenzione di denominazione 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 dell'SVM, %V è il volume di origine e %N è il nome del nodo di destinazione della topologia.

Se il valore immesso non è valido, il campo della convenzione di denominazione viene evidenziato in rosso. Facendo clic sul collegamento “Anteprima nome” viene visualizzata un’anteprima della convenzione di denominazione immessa; il testo dell’anteprima si aggiorna dinamicamente man mano che si digita una convenzione di denominazione nel campo di testo. Quando viene creata la relazione, al nome della destinazione viene aggiunto un suffisso compreso tra 001 e 999, in sostituzione del suffisso nnn visualizzato nel testo di anteprima, con 001 assegnato per primo, 002 assegnato per secondo e così via.

• Impostazioni della relazione

Consente di specificare la velocità di trasferimento massima, la politica SnapMirror e la pianificazione utilizzata dalla relazione di protezione:

- Velocità massima di trasferimento

Specifica la velocità massima alla quale i dati vengono trasferiti tra cluster sulla rete. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di base tra le relazioni è illimitato.

- Politica SnapMirror

Specifica la policy ONTAP SnapMirror per la relazione. L'impostazione predefinita è DPDefault.

- Crea politica

Avvia la finestra di dialogo Crea criterio SnapMirror , che consente di creare e utilizzare un nuovo criterio SnapMirror .

- Programma SnapMirror

Specifica la policy ONTAP SnapMirror per la relazione. Le pianificazioni disponibili includono Nessuna, 5 minuti, 8 ore, giornaliera, oraria e settimanale. L'impostazione predefinita è Nessuno, a indicare che alla relazione non è associata alcuna pianificazione. Le relazioni senza pianificazioni non hanno valori di stato di ritardo, a meno che non appartengano a un servizio di archiviazione.

- Crea programma

Avvia la finestra di dialogo Crea pianificazione, che consente di creare una nuova pianificazione SnapMirror .

Scheda SnapVault

Consente di specificare un cluster secondario, SVM e aggregato per una relazione di protezione, nonché una convenzione di denominazione per i volumi secondari durante la creazione di una relazione SnapVault . È anche possibile specificare una politica e una pianificazione SnapVault .

• Vista topologica

Visualizza una rappresentazione visiva della relazione che stai creando. Per impostazione predefinita, la risorsa secondaria SnapVault nella topologia è evidenziata.

• Informazioni secondarie

Consente di selezionare le risorse secondarie per una relazione di protezione:

- Collegamento avanzato

Avvia la finestra di dialogo Impostazioni secondarie avanzate.

- Grappolo

Elenca i cluster disponibili come host di protezione secondari. Questo campo è obbligatorio.

- macchina virtuale di archiviazione (SVM)

Elenca le SVM disponibili sul cluster selezionato. È necessario selezionare un cluster prima che l'elenco SVM venga popolato. Questo campo è obbligatorio.

- Aggregato

Elenca gli aggregati disponibili sull'SVM selezionato. È necessario selezionare un cluster prima che l'elenco Aggregato venga compilato. Questo campo è obbligatorio. L'elenco Aggregato visualizza le seguenti informazioni:

- Rango

Quando più aggregati soddisfano tutti i requisiti per una destinazione, il rango indica la priorità in cui l'aggregato è elencato, in base alle seguenti condizioni:

- A. Per consentire la separazione del dominio di errore, è preferibile un aggregato posizionato su un nodo diverso dal nodo del volume primario.
- B. È preferibile un aggregato su un nodo con meno volumi per consentire il bilanciamento del carico tra i nodi di un cluster.
- C. Per consentire il bilanciamento della capacità, è preferibile un aggregato che abbia più spazio libero rispetto ad altri aggregati. Un grado pari a 1 significa 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 denominazione

Specifica la convenzione di denominazione predefinita applicata al volume secondario. È possibile accettare la convenzione di denominazione 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 dell'SVM, %V è il volume di origine e %N è il nome del nodo secondario della topologia.

Se il valore immesso non è valido, il campo della convenzione di denominazione viene evidenziato in rosso. Facendo clic sul collegamento "Anteprima nome" viene visualizzata un'anteprima della convenzione di denominazione immessa; il testo dell'anteprima si aggiorna dinamicamente man mano che si digita una convenzione di denominazione nel campo di testo. Se si digita un valore non valido, le informazioni non valide vengono visualizzate come punti interrogativi rossi nell'area di anteprima. Quando si crea la relazione, al nome secondario viene aggiunto un suffisso compreso tra 001 e 999, sostituendo il nnn visualizzato nel testo di anteprima, con 001 assegnato per primo, 002 assegnato per secondo e così via.

- **Impostazioni della relazione**

Consente di specificare la velocità di trasferimento massima, la politica SnapVault e la pianificazione SnapVault utilizzate dalla relazione di protezione:

- Velocità massima di trasferimento

Specifica la velocità massima alla quale i dati vengono trasferiti tra cluster sulla rete. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di base tra le relazioni è illimitato.

- Politica SnapVault

Specifica la policy ONTAP SnapVault per la relazione. L'impostazione predefinita è XDPDefault.

- Crea politica

Avvia la finestra di dialogo Crea criterio SnapVault , che consente di creare e utilizzare un nuovo criterio SnapVault .

- Programma SnapVault

Specifica la pianificazione ONTAP SnapVault per la relazione. Le pianificazioni disponibili includono Nessuna, 5 minuti, 8 ore, giornaliera, oraria e settimanale. L'impostazione predefinita è Nessuno, a indicare che alla relazione non è associata alcuna pianificazione. Le relazioni senza pianificazioni non hanno valori di stato di ritardo, a meno che non appartengano a un servizio di archiviazione.

- Crea programma

Avvia 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 attività:

- **Cancellare**

Annulla le selezioni e chiude la finestra di dialogo Configura protezione.

- **Fare domanda a**

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 relazioni 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 è possibile creare una pianificazione meno frequente quando i dati cambiano raramente.

Non è possibile configurare le pianificazioni per le relazioni sincrone SnapMirror .

- **Cluster di destinazione**

Il nome del cluster selezionato nella scheda SnapVault o nella scheda SnapMirror della finestra di dialogo Configura protezione.

- **Nome programma**

Il nome che fornisci per la pianificazione. I nomi delle pianificazioni possono essere composti dai caratteri dalla A alla Z, dalla a alla z, dallo 0 al 9, nonché da uno qualsiasi dei seguenti caratteri speciali: ! @ # \$ % {accento circonflesso} & * () _ -. I nomi degli orari non possono contenere i seguenti caratteri: < >.

- **Base o Avanzato**

La modalità di pianificazione che desideri utilizzare.

La modalità base include i seguenti elementi:

- Ripetere

Con quale frequenza si verifica un trasferimento programmato. Le opzioni disponibili sono oraria, giornaliera e settimanale.

- Giorno

Quando si seleziona una ripetizione settimanale, il giorno della settimana in cui avviene il trasferimento.

- Tempo

Selezionando Giornaliero o Settimanale, viene indicata l'ora del giorno in cui avviene il trasferimento.

La modalità avanzata include i seguenti elementi:

- Mesi

Un elenco numerico separato da virgole che rappresenta i mesi dell'anno. I valori validi sono compresi tra 0 e 11, dove zero rappresenta gennaio e così via. Questo elemento è facoltativo. Lasciando il campo vuoto si intende che i trasferimenti avvengono ogni mese.

- Giorni

Un elenco numerico separato da virgole che rappresenta il giorno del mese. I valori validi sono compresi tra 1 e 31. Questo elemento è facoltativo. Lasciando il campo vuoto si implica 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 compresi tra 0 e 6, dove 0 rappresenta la domenica e così via. Questo elemento è facoltativo. Lasciando il campo vuoto si implica 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 nel giorno della settimana specificato e non tutti i giorni.

- Ore

Un elenco numerico separato da virgole che rappresenta il numero di ore in un giorno. I valori validi sono compresi tra 0 e 23, dove 0 rappresenta la mezzanotte. Questo elemento è facoltativo.

- Minuti

Un elenco numerico separato da virgole che rappresenta i minuti in un'ora. I valori validi sono compresi tra 0 e 59. Questo elemento è obbligatorio.

Finestra di dialogo Crea criterio SnapMirror

La finestra di dialogo Crea criterio SnapMirror consente di creare un criterio per impostare la priorità per i trasferimenti SnapMirror. Si utilizzano policy 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.

- **Destinazione SVM**

Il nome dell'SVM selezionato nella scheda SnapMirror della finestra di dialogo Configura protezione.

- **Nome della polizza**

Il nome che fornisci per la nuova polizza. I nomi delle policy possono essere composti dai caratteri dalla A alla Z, dalla a alla z, dallo 0 al 9, dal punto (.), dal trattino (-) e dal carattere di sottolineatura (_).

- **Priorità di trasferimento**

Priorità con cui viene eseguito un trasferimento per operazioni asincrone. È possibile selezionare Normale o Basso. Le relazioni di trasferimento con policy che specificano una priorità di trasferimento normale vengono eseguite prima di quelle con policy che specificano una priorità di trasferimento bassa.

- **Commento**

Campo facoltativo in cui è possibile aggiungere commenti sulla policy.

- **Riavvio del trasferimento**

Indica quale azione di riavvio intraprendere quando un trasferimento viene interrotto da un'operazione di annullamento o da qualsiasi tipo di errore, come un'interruzione della rete. Puoi 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 attività:

- **Cancellare**

Annulla le selezioni e chiude la finestra di dialogo Configura protezione.

- **Fare domanda a**

Applica le selezioni e avvia il processo di protezione.

Finestra di dialogo Crea criterio SnapVault

La finestra di dialogo Crea criterio SnapVault consente di creare un criterio per impostare la priorità per i trasferimenti SnapVault. Si utilizzano policy per massimizzare l'efficienza dei trasferimenti dal volume primario a quello secondario.

- **Cluster di destinazione**

Il nome del cluster selezionato nella scheda SnapVault della finestra di dialogo Configura protezione.

- **Destinazione SVM**

Il nome dell'SVM selezionato nella scheda SnapVault della finestra di dialogo Configura protezione.

- **Nome della polizza**

Il nome che fornisci per la nuova polizza. I nomi delle policy possono essere composti dai caratteri dalla A alla Z, dalla a alla z, dallo 0 al 9, dal punto (.), dal trattino (-) e dal carattere di sottolineatura (_).

- **Priorità di trasferimento**

La priorità con cui viene eseguito il trasferimento. È possibile selezionare Normale o Basso. Le relazioni di trasferimento con policy che specificano una priorità di trasferimento normale vengono eseguite prima di quelle con policy che specificano una priorità di trasferimento bassa. L'impostazione predefinita è Normale.

- **Commento**

Un campo facoltativo in cui puoi aggiungere un commento di massimo 255 caratteri sulla policy SnapVault.

- **Ignora tempo di accesso**

Specifica se i trasferimenti incrementali vengono ignorati per i file di cui è stato modificato solo l'orario di accesso.

- **Etichetta di replicazione**

Elenca in una tabella le regole associate alle copie Snapshot selezionate da ONTAP che hanno un'etichetta di replica specifica in una policy. Sono inoltre disponibili le seguenti informazioni e azioni:

- Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti azioni:

- Aggiungere

Consente di creare un'etichetta di copia Snapshot e un conteggio di conservazione.

- **Modifica conteggio conservazione**

Consente di modificare il conteggio di conservazione per un'etichetta di copia Snapshot esistente. Il conteggio della conservazione deve essere un numero 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 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 nella policy. Se selezioni più volumi che hanno due o più criteri di copia Snapshot locali, la tabella visualizza tutte le etichette di tutti i criteri

- **Programma**

Visualizza la pianificazione associata a ciascuna etichetta di copia Snapshot. Se a un'etichetta sono associate più pianificazioni, le pianificazioni per quell'etichetta vengono visualizzate in un elenco separato da virgole. Se si selezionano più volumi con la stessa etichetta ma con pianificazioni diverse, nella pianificazione viene visualizzato "Varie" per indicare che ai volumi selezionati è associata più di una pianificazione.

- **Conteggio della conservazione della destinazione**

Visualizza il numero di copie Snapshot con l'etichetta specificata conservate sullo SnapVault secondario. I conteggi di conservazione per le etichette con più pianificazioni visualizzano la somma dei conteggi di conservazione di ciascuna coppia etichetta-pianificazione. Se si selezionano più volumi con due o più criteri di copia Snapshot locali, il conteggio della conservazione è vuoto.

Finestra di dialogo Modifica relazione

È possibile modificare una relazione di protezione esistente per cambiare la velocità di trasferimento massima, la politica di protezione o la pianificazione della protezione.

Informazioni sulla destinazione

- **Cluster di destinazione**

Nome del cluster di destinazione selezionato.

- **Destinazione SVM**

Il nome dell'SVM selezionato

- **Impostazioni della relazione**

Consente di specificare la velocità di trasferimento massima, la politica SnapMirror e la pianificazione utilizzata dalla relazione di protezione:

- **Velocità massima di trasferimento**

Specifica la velocità massima alla quale i dati di base 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 quindi selezionare kilobyte al secondo (KBps), megabyte al secondo (MBps), gigabyte al secondo (GBps) o terabyte al secondo (TBps). La velocità di trasferimento massima specificata deve essere maggiore di 1 KBps e minore di 4 TBps. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di base tra le relazioni è illimitato. Se il cluster primario e quello secondario sono uguali, questa impostazione è disabilitata.

- **Politica SnapMirror**

Specifica la policy ONTAP SnapMirror per la relazione. L'impostazione predefinita è DPDefault.

- **Crea politica**

Avvia la finestra di dialogo Crea criterio SnapMirror , che consente di creare e utilizzare un nuovo criterio SnapMirror .

- **Programma SnapMirror**

Specifica la policy ONTAP SnapMirror per la relazione. Le pianificazioni disponibili includono Nessuna, 5 minuti, 8 ore, giornaliera, oraria e settimanale. L'impostazione predefinita è Nessuno, a indicare che alla relazione non è associata alcuna pianificazione. Le relazioni senza pianificazioni non hanno valori di stato di ritardo, a meno che non appartengano a un servizio di archiviazione.

- **Crea programma**

Avvia la finestra di dialogo Crea pianificazione, che consente di creare una nuova pianificazione SnapMirror .

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Cancellare**

Annulla 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 Inizializza/Aggiorna

La finestra di dialogo Inizializza/Aggiorna consente di eseguire un primo trasferimento di base su una nuova relazione di protezione oppure di aggiornare una relazione se è già inizializzata e si desidera eseguire un aggiornamento incrementale manuale e non pianificato.

Scheda Opzioni di trasferimento

La scheda Opzioni di trasferimento consente di modificare la priorità di inizializzazione di un trasferimento e di modificare la larghezza di banda utilizzata durante i trasferimenti.

- **Priorità di trasferimento**

La priorità con cui viene eseguito il trasferimento. È possibile selezionare Normale o Basso. Le relazioni con policy che specificano una priorità di trasferimento normale vengono eseguite prima di quelle che specificano una priorità di trasferimento bassa. Per impostazione predefinita è selezionata l'opzione Normale.

- **Velocità di trasferimento massima**

Specifica la velocità massima alla quale i dati vengono trasferiti tra cluster sulla rete. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di base 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 di velocità di trasferimento massima:

- Utilizzare i valori specificati durante la configurazione o la modifica della relazione individuale

Se 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.

- Illimitato

Indica che non vi è alcuna limitazione di larghezza di banda per i trasferimenti tra relazioni. Questo campo è disponibile solo quando vengono inizializzate o aggiornate più relazioni con velocità di trasferimento diverse.

- Limita 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 quindi selezionare kilobyte al secondo (KBps), megabyte al secondo (MBps), gigabyte al secondo (GBps) o terabyte al secondo (TBps). La velocità di trasferimento massima specificata deve essere maggiore di 1 KBps e minore di 4 TBps.

Scheda Copie snapshot di origine

La scheda Copie snapshot di origine visualizza le seguenti informazioni sulla copia snapshot di origine utilizzata per il trasferimento di base:

- **Volume sorgente**

Visualizza i nomi dei volumi sorgente corrispondenti.

- **Volume di destinazione**

Visualizza i nomi dei volumi di destinazione selezionati.

- **Tipo di fonte**

Visualizza il tipo di volume. Il tipo può essere Lettura/scrittura o Protezione dati.

- **Copia istantanea**

Visualizza la copia Snapshot utilizzata per il trasferimento dei dati. Facendo clic sul valore Copia snapshot viene visualizzata la finestra di dialogo 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 di cui si dispone e dell'operazione che si sta eseguendo. L'opzione per specificare una copia Snapshot diversa non

è disponibile per le origini di tipo protezione dati.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Cancellare**

Annulla 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 Risincronizza

La finestra di dialogo Risincronizza consente di risincronizzare i dati su una relazione SnapMirror o SnapVault precedentemente interrotta e in seguito trasformata in un volume di lettura/scrittura. È anche possibile risincronizzare quando una copia Snapshot comune richiesta sul volume di origine viene eliminata, causando il fallimento degli aggiornamenti 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 di trasferimento**

La priorità con cui viene eseguito il trasferimento. È possibile selezionare Normale o Basso. Le relazioni con policy che specificano una priorità di trasferimento normale vengono eseguite prima di quelle con policy che specificano una priorità di trasferimento bassa.

- **Velocità di trasferimento massima**

Specifica la velocità massima alla quale 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 quindi selezionare kilobyte al secondo (KBps), megabyte al secondo (MBps), gigabyte al secondo (GBps) o TBps. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di base tra le relazioni è illimitato.

Scheda Copie snapshot di origine

La scheda Copie snapshot di origine visualizza le seguenti informazioni sulla copia snapshot di origine utilizzata per il trasferimento di base:

- **Volume sorgente**

Visualizza i nomi dei volumi sorgente corrispondenti.

- **Volume di destinazione**

Visualizza i nomi dei volumi di destinazione selezionati.

- **Tipo di fonte**

Visualizza il tipo di volume: Lettura/scrittura o Protezione dati.

- **Copia istantanea**

Visualizza la copia Snapshot utilizzata per il trasferimento dei dati. Facendo clic sul valore Copia snapshot viene visualizzata la finestra di dialogo 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 e dell'operazione che si sta eseguendo.

Pulsanti di comando

- **Invia**

Avvia il processo di risincronizzazione e chiude la finestra di dialogo Risincronizza.

- **Cancellare**

Annulla le selezioni e chiude la finestra di dialogo Risincronizza.

Finestra di dialogo Seleziona copia snapshot sorgente

Utilizzare la finestra di dialogo Seleziona copia snapshot di origine per selezionare una copia snapshot specifica per trasferire i dati tra relazioni di protezione oppure selezionare il comportamento predefinito, che varia a seconda che si stia inizializzando, aggiornando o risincronizzando una relazione e che la relazione sia uno SnapMirror o SnapVault.

Predefinito

Consente di selezionare il comportamento predefinito per determinare quale copia Snapshot viene utilizzata per inizializzare, aggiornare e risincronizzare i trasferimenti per le relazioni SnapVault e SnapMirror .

Se si esegue un trasferimento SnapVault , il comportamento predefinito per ciascuna operazione è il seguente:

Operazione	Comportamento predefinito SnapVault quando la sorgente è in lettura/scrittura	Comportamento predefinito SnapVault quando l'origine è Data Protection (DP)
Inizializzare	Crea una nuova copia Snapshot e la trasferisce.	Trasferisce l'ultima copia Snapshot esportata.
Aggiornamento	Trasferisce solo copie Snapshot etichettate, come specificato nella policy.	Trasferisce l'ultima copia Snapshot esportata.
Risincronizzare	Trasferisce tutte le copie Snapshot etichettate create dopo la copia Snapshot comune più recente.	Trasferisce la copia Snapshot etichettata più recente.

Se si esegue un trasferimento SnapMirror , il comportamento predefinito per ciascuna operazione è il seguente:

Operazione	Comportamento predefinito SnapMirror	Comportamento predefinito SnapMirror quando la relazione è il secondo salto in una cascata SnapMirror a SnapMirror
Inizializzare	Crea una nuova copia Snapshot e trasferisce questa e tutte le copie Snapshot create prima della nuova copia Snapshot.	Trasferisce tutte le copie Snapshot dalla sorgente.
Aggiornamento	Crea una nuova copia Snapshot e trasferisce questa e tutte le copie Snapshot create prima della nuova copia Snapshot.	Trasferisce tutte le copie Snapshot.
Risincronizzare	Crea una nuova copia Snapshot e quindi trasferisce tutte le copie Snapshot dalla sorgente.	Trasferisce tutte le copie Snapshot dal volume secondario al volume terziario 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 la selezione della copia Snapshot è consentita per tale operazione.

- **Copia istantanea**

Visualizza le copie Snapshot esistenti tra cui è possibile selezionare un trasferimento.

- **Data di creazione**

Visualizza la data e l'ora in cui è stata creata la copia Snapshot. Le copie snapshot sono elencate dalla più recente alla meno recente, con la più recente in cima all'elenco.

Se si esegue un trasferimento SnapVault e si desidera selezionare una copia Snapshot esistente da trasferire da un'origine a una destinazione, il comportamento per ciascuna operazione è il seguente:

Operazione	Comportamento SnapVault quando si specifica una copia Snapshot	Comportamento 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 dati.
Aggiornamento	Trasferisce la copia Snapshot specificata.	La selezione della copia snapshot di origine non è supportata per i volumi di protezione dati.

Operazione	Comportamento SnapVault quando si specifica una copia Snapshot	Comportamento SnapVault quando si specifica una copia Snapshot in una cascata
Risincronizzare	Trasferisce la copia Snapshot selezionata.	La selezione della copia snapshot di origine non è supportata per i volumi di protezione dati.

Se si esegue un trasferimento SnapMirror e si desidera selezionare una copia Snapshot esistente da trasferire da un'origine a una destinazione, il comportamento per ciascuna operazione è il seguente:

Operazione	Comportamento SnapMirror quando si specifica una copia Snapshot	Comportamento SnapMirror quando si specifica una copia Snapshot in una cascata
Inizializzare	Trasferisce tutte le copie Snapshot sulla sorgente, fino alla copia Snapshot specificata.	La selezione della copia snapshot di origine non è supportata per i volumi di protezione dati.
Aggiornamento	Trasferisce tutte le copie Snapshot sulla sorgente, fino alla copia Snapshot specificata.	La selezione della copia snapshot di origine non è supportata per i volumi di protezione 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 dati.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività:

- **Invia**

Invia le selezioni e chiude la finestra di dialogo Seleziona copia snapshot di origine.

- **Cancellare**

Annulla le selezioni e chiude la finestra di dialogo Seleziona copia snapshot di origine.

Finestra di dialogo Risincronizzazione inversa

Quando una relazione di protezione viene interrotta perché il volume di origine è disabilitato e la destinazione è diventata un 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 disabilita il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per gestire i dati convertendoli 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 rispetto ai dati sulla copia Snapshot comune vengono eliminati.

Prima della risincronizzazione inversa

Visualizza l'origine e la destinazione di una relazione prima di un'operazione di risincronizzazione inversa.

- **Volume sorgente**

Nome e posizione del volume di origine prima di un'operazione di risincronizzazione inversa.

- **Volume di destinazione**

Nome e posizione del volume di destinazione prima di un'operazione di risincronizzazione inversa.

Dopo la risincronizzazione inversa

Visualizza l'origine e la destinazione di una relazione dopo un'operazione di risincronizzazione di riserva.

- **Volume sorgente**

Nome e posizione del volume sorgente dopo un'operazione di risincronizzazione inversa.

- **Volume di destinazione**

Nome e posizione del volume di destinazione dopo un'operazione di risincronizzazione inversa.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti azioni:

- **Invia**

Avvia il processo di risincronizzazione inversa.

- **Cancellare**

Chiude la finestra di dialogo Risincronizzazione inversa senza avviare un'operazione di risincronizzazione inversa.

Relazione: visualizzazione di tutte le relazioni

La vista Relazione: tutte le relazioni mostra informazioni sulle relazioni di protezione nel sistema di archiviazione.

Per impostazione predefinita, quando si accede alla pagina Relazioni, il report visualizzato include le relazioni di protezione di livello superiore sia per i volumi che per le VM di archiviazione. I controlli nella parte superiore della pagina consentono di selezionare una vista specifica, eseguire ricerche per individuare oggetti specifici, creare e applicare filtri per restringere l'elenco dei dati visualizzati, aggiungere/rimuovere/riordinare colonne nella pagina ed esportare i dati nella pagina in un file .csv, .pdf o .xlsx. Dopo aver personalizzato la pagina, puoi salvare i risultati come visualizzazione personalizzata e quindi programmare la generazione e l'invio periodico tramite e-mail di un report di questi dati. Per impostazione predefinita, quando si seleziona il menu **Relazioni**, il report visualizzato include le relazioni di protezione sia per i volumi che per le VM di archiviazione nel data center. È possibile utilizzare l'opzione **Filtro** per visualizzare solo i sistemi di archiviazione selezionati,

ad esempio solo i volumi o solo le VM di archiviazione. Lo stesso report viene visualizzato nella pagina Archiviazione e solo per l'entità di archiviazione selezionata. Se si desidera visualizzare le relazioni tra volumi o VM di archiviazione, è possibile accedere alla pagina **Archiviazione > Volumi > Relazione: tutte le relazioni** oppure accedere a **Protezione > Relazioni > Relazione: tutte le relazioni** e utilizzare l'opzione **Tipo di oggetto relazione** in **Filtro** per filtrare solo i dati dei volumi o delle VM di archiviazione.

La pagina Relazioni che elenca tutte le relazioni di protezione contiene il collegamento **Visualizza in System Manager** per il cluster di destinazione, che consente di visualizzare gli stessi oggetti in ONTAP System Manager.

- **Stato**

Visualizza lo stato attuale della relazione di protezione.

Lo stato può essere uno di Errore () , Avvertimento () , oppure OK () .

- **VM di archiviazione di origine**

Visualizza il nome dell'SVM di origine. È possibile visualizzare maggiori dettagli sull'SVM di origine facendo clic sul nome dell'SVM.

Se un SVM è presente nel cluster ma non è ancora stato aggiunto all'inventario di Unified Manager, oppure se l'SVM è stato creato dopo l'ultimo aggiornamento del cluster, questo campo sarà vuoto. È necessario assicurarsi che l'SVM esista oppure eseguire una nuova individuazione sul cluster per aggiornare l'elenco delle risorse.

- **Fonte**

Visualizza il volume di origine o la VM di archiviazione di origine protetta in base alla selezione effettuata. È possibile visualizzare maggiori dettagli sul volume di origine o sulla VM di archiviazione facendo clic sul nome del volume o della VM di archiviazione.

Se il messaggio `Resource-key not discovered` viene visualizzato, ciò potrebbe indicare che il volume esiste nel cluster ma non è ancora stato aggiunto all'inventario di Unified Manager oppure che il volume è stato creato dopo l'ultimo aggiornamento del cluster. È necessario assicurarsi che il volume esista oppure eseguire una nuova individuazione sul cluster per aggiornare l'elenco delle risorse.

- **VM di archiviazione di destinazione**

Visualizza il nome dell'SVM di destinazione. È possibile visualizzare maggiori dettagli sull'SVM di destinazione facendo clic sul nome dell'SVM.

- **Destinazione**

Visualizza il nome del volume di destinazione o della VM di archiviazione in base alla selezione effettuata. È possibile visualizzare maggiori dettagli sul volume di destinazione o sulla VM di archiviazione facendo clic sul nome dell'oggetto corrispondente.

- **Tipo di oggetto relazione**

Visualizza il tipo di oggetto utilizzato nella relazione, ad esempio VM di archiviazione, 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 esse si accede alla pagina LUN per visualizzare la relazione.

• Politica

Visualizza il nome del criterio di protezione per la relazione SnapMirror . È possibile fare clic sul nome della policy per visualizzare i dettagli associati a tale policy, tra cui le seguenti informazioni:

- Priorità di trasferimento

Specifica la priorità con cui viene eseguito un trasferimento per le operazioni asincrone. La priorità di trasferimento è Normale o Bassa. I trasferimenti con priorità normale vengono programmati prima dei trasferimenti con priorità bassa. L'impostazione predefinita è Normale.

- Ignora tempo di accesso

Si applica solo alle relazioni SnapVault . Specifica se i trasferimenti incrementali ignorano i file di cui è stato modificato solo l'orario di accesso. I valori sono Vero o Falso. Il valore predefinito è False.

- Quando la relazione non è sincronizzata

Specifica l'azione che ONTAP esegue quando una relazione sincrona non può essere sincronizzata. Le relazioni StrictSync limiteranno l'accesso al volume primario in caso di errore di sincronizzazione con il volume secondario. Le relazioni di sincronizzazione non limitano l'accesso al primario se si verifica un errore di 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 commenti specifici sulla policy selezionata.

- Etichetta SnapMirror

Specifica l'etichetta SnapMirror per la prima pianificazione associata al criterio di copia Snapshot. L'etichetta SnapMirror viene utilizzata dal sottosistema SnapVault quando si esegue il backup di copie Snapshot in una destinazione SnapVault .

- Impostazione di conservazione

Specifica per quanto tempo vengono conservati i backup, in base al tempo o al numero di backup.

- Copie istantanee effettive

Specifica il numero di copie Snapshot su questo volume che corrispondono all'etichetta specificata.

- Conserva le copie snapshot

Specifica il numero di copie SnapVault Snapshot che non vengono eliminate automaticamente anche se viene raggiunto il limite massimo per il criterio. I valori sono Vero o Falso. Il valore predefinito è False.

- Soglia di avviso di conservazione

Specifica il limite di copie Snapshot raggiunto il quale viene inviato un avviso per indicare che il limite massimo di conservazione è quasi raggiunto.

- **Durata del ritardo**

Visualizza il ritardo temporale dei dati sullo specchio rispetto alla sorgente.

La durata del ritardo dovrebbe essere prossima o uguale a 0 secondi per le relazioni StrictSync.

- **Stato di ritardo**

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.

- Avvertimento

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 alle relazioni sincrone perché non è possibile configurare una pianificazione.

- **Ultimo aggiornamento riuscito**

Visualizza l'ora dell'ultima operazione SnapMirror o SnapVault riuscita.

L'ultimo aggiornamento riuscito non è applicabile alle relazioni sincrone.

- **Relazioni costituenti**

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:

- Specchio asincrono
 - Vault asincrono
 - MirrorVault asincrono
 - Sincronizzazione rigorosa
 - Sincronizzazione

- **Stato del trasferimento**

Visualizza lo stato del trasferimento per la relazione di protezione. Lo stato del trasferimento può essere uno dei seguenti:

- Aborto

I trasferimenti SnapMirror sono abilitati; tuttavia, è in corso un'operazione di interruzione del trasferimento che potrebbe includere la rimozione del checkpoint.

- Controllo

Il volume di destinazione è sottoposto a un controllo diagnostico e non è in corso alcun trasferimento.

- Finalizzazione

I trasferimenti SnapMirror sono abilitati. Il volume è attualmente nella fase di post-trasferimento per trasferimenti incrementali SnapVault .

- Oziare

I trasferimenti sono abilitati e non è in corso alcun trasferimento.

- Sincronizzato

I dati nei due volumi nella relazione sincrona sono sincronizzati.

- Fuori sincrono

I dati nel volume di destinazione non sono sincronizzati con il volume di origine.

- Preparazione

I trasferimenti SnapMirror sono abilitati. Il volume è attualmente nella fase di pre-trasferimento per trasferimenti incrementali SnapVault .

- In coda

I trasferimenti SnapMirror sono abilitati. Non sono in corso trasferimenti.

- Quieced

I trasferimenti SnapMirror sono disabilitati. Nessun trasferimento in corso.

- Quiescenza

È in corso un trasferimento SnapMirror . I trasferimenti aggiuntivi sono disabilitati.

- Trasferimento

I trasferimenti SnapMirror sono abilitati e un trasferimento è in corso.

- Transizione

Il trasferimento asincrono dei dati dal volume di origine a quello di destinazione è completo e la transizione al funzionamento sincrono è iniziata.

- In attesa

È stato avviato un trasferimento SnapMirror , ma alcune attività associate sono in attesa di essere messe in coda.

- **Durata dell'ultimo trasferimento**

Visualizza il tempo impiegato per completare l'ultimo trasferimento dati.

La durata del trasferimento non è applicabile alle relazioni StrictSync perché il trasferimento deve essere simultaneo.

- **Ultima dimensione del trasferimento**

Visualizza la dimensione, in byte, dell'ultimo trasferimento dati.

La dimensione del trasferimento non è applicabile alle relazioni StrictSync.

- **Mediatori**

Visualizza lo stato del mediatore.

- Non applicabile

Se il cluster non supporta la sincronizzazione attiva SnapMirror .

- Non configurato

Se non è configurato, oppure 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 sia i cluster di origine che quelli 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 viene selezionato un volume sorgente, lo stato della relazione non è applicabile e non viene visualizzato.

- **Salute delle relazioni**

Visualizza lo stato della relazione del cluster.

- **Motivo malsano**

Il motivo per cui la relazione non è sana.

- **Priorità di trasferimento**

Visualizza la priorità con cui viene eseguito un trasferimento. La priorità di trasferimento è Normale o Bassa. I trasferimenti con priorità normale vengono programmati prima dei trasferimenti con priorità bassa.

La priorità di trasferimento non è applicabile alle relazioni sincrone perché tutti i trasferimenti vengono trattati con la stessa priorità.

- **Programma**

Visualizza il nome della pianificazione di protezione assegnata alla relazione.

Il programma non è applicabile alle relazioni sincrone.

- **Replica flessibile della versione**

Visualizza Sì, Sì con opzione di backup o Nessuno.

- **Cluster di origine**

Visualizza il nome di dominio completo (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 sorgente**

Visualizza il nome del collegamento al nome del nodo di origine per la relazione SnapMirror di un volume e visualizza il collegamento al conteggio dei nodi della relazione SnapMirror quando l'oggetto è una VM di archiviazione o un gruppo di coerenza.

Nella visualizzazione personalizzata, quando si fa clic sul collegamento del nome del nodo, è possibile visualizzare ed estendere la protezione per gli oggetti di archiviazione sui quali i volumi di tali gruppi di coerenza appartengono a una relazione di sincronizzazione attiva SnapMirror .

Facendo clic sul collegamento del conteggio dei nodi, si accede alla pagina dei nodi con i rispettivi nodi associati a quella relazione. Quando il conteggio dei nodi è 0, non viene visualizzato alcun valore poiché non ci sono nodi associati alla relazione.

- **Nodo di destinazione**

Visualizza il nome del collegamento al nome del nodo di destinazione per la relazione SnapMirror di un volume e visualizza il collegamento al conteggio dei nodi della relazione SnapMirror quando l'oggetto è una VM di archiviazione o un gruppo di coerenza.

Facendo clic sul collegamento del conteggio dei nodi, si accede alla pagina dei nodi con i rispettivi nodi associati a quella relazione. Quando il conteggio dei nodi è 0, non viene visualizzato alcun valore poiché non ci sono nodi associati alla relazione.

- **Cluster di destinazione**

Visualizza il nome del cluster di destinazione per la relazione SnapMirror .

- **FQDN del cluster di destinazione**

Visualizza il nome di dominio completo (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 tra volumi e gruppi di coerenza per l'ordine dei cluster e delle macchine virtuali di storage, tra cui:

- SnapMirror
- VM di archiviazione DR
- SnapMirror, Storage VM DR

- Gruppo di coerenza
- SnapMirror, Gruppo di coerenza.

Informazioni correlate

- Per informazioni sulla visualizzazione **Relazione: MetroCluster**, vedere ["Monitoraggio delle configurazioni MetroCluster"](#) .
- Per informazioni sulla visualizzazione **Relazione: Stato del trasferimento dell'ultimo mese**, vedere ["Relazione: Visualizzazione dello stato del trasferimento dell'ultimo mese"](#) .
- Per informazioni sulla visualizzazione **Relazione: Tutte le relazioni**, vedere ["Relazione: Visualizzazione del tasso di trasferimento dell'ultimo mese"](#) .

Relazione: Visualizzazione dello stato del trasferimento dell'ultimo mese

La vista Relazione: Stato del trasferimento dell'ultimo mese consente di analizzare le tendenze di trasferimento in un determinato periodo di tempo per volumi e VM di archiviazione in relazioni asincrone. Questa pagina mostra anche se il trasferimento è riuscito o meno.

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 colonne sulla pagina ed esportare i dati sulla pagina in un .csv , .pdf , O .xlsx file. Dopo aver personalizzato la pagina, puoi salvare i risultati come visualizzazione personalizzata e quindi programmare la generazione e l'invio periodico tramite e-mail di un report di questi dati. È possibile utilizzare l'opzione **Filtro** per visualizzare solo i sistemi di archiviazione selezionati, ad esempio solo i volumi o solo le VM di archiviazione. Lo stesso report viene visualizzato nella pagina Archiviazione e solo per l'entità di archiviazione selezionata. Ad esempio, se si desidera visualizzare le relazioni tra volumi, è possibile accedere al report Relazione: Stato trasferimento ultimo mese per le VM di archiviazione dal menu **Archiviazione > VM di archiviazione > Relazione: Stato trasferimento ultimo mese** oppure dal menu **Protezione > Relazioni > Relazione: Stato trasferimento ultimo mese** e utilizzare il **Filtro** per visualizzare solo i dati per i volumi.

- **Volume sorgente**

Visualizza il nome del volume sorgente.

- **Volume di destinazione**

Visualizza il nome del volume di destinazione.

- **Tipo di operazione**

Visualizza il tipo di trasferimento del volume.

- **Risultato dell'operazione**

Indica se il trasferimento del volume è riuscito.

- **Ora di inizio del trasferimento**

Visualizza l'ora di inizio del trasferimento del volume.

- **Ora di fine trasferimento**

Visualizza l'ora di fine del trasferimento del volume.

- **Durata del trasferimento**

Visualizza il tempo impiegato (in ore) per completare il trasferimento del volume.

- **Dimensione del trasferimento**

Visualizza la dimensione (in MB) del volume trasferito.

- **Fonte SVM**

Visualizza il nome della macchina virtuale di archiviazione (SVM).

- **Cluster di origine**

Visualizza il nome del cluster di origine.

- **Destinazione SVM**

Visualizza il nome della SVM di destinazione.

- **Cluster di destinazione**

Visualizza il nome del cluster di destinazione.

Informazioni correlate

- Per informazioni sulla visualizzazione **Relazione: Tutte le relazioni**, vedere "[Relazione: visualizzazione di tutte le relazioni](#)".
- Per informazioni sulla visualizzazione **Relazione: MetroCluster**, vedere "[Monitoraggio delle configurazioni MetroCluster](#)".
- Per informazioni sulla visualizzazione **Relazione: Tutte le relazioni**, vedere "[Relazione: Visualizzazione del tasso di trasferimento dell'ultimo mese](#)".

Relazione: Visualizzazione del tasso di trasferimento dell'ultimo mese

La vista Relazione: Velocità di trasferimento dell'ultimo mese consente di analizzare la quantità di volume di dati trasferito quotidianamente per i volumi in relazioni asincrone. Questa pagina fornisce anche dettagli sui trasferimenti giornalieri e sul tempo necessario per completare l'operazione di trasferimento per volumi e VM di archiviazione.

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 colonne nella pagina ed esportare i dati nella pagina in un file .csv, .pdf o .xlsx. Dopo aver personalizzato la pagina, puoi salvare i risultati come visualizzazione personalizzata e quindi programmare la generazione e l'invio periodico tramite e-mail di un report di questi dati. Ad esempio, se si desidera visualizzare le relazioni tra volumi, è possibile accedere al menu **Archiviazione > Volumi > Relazione: Velocità di trasferimento ultimo mese** oppure accedere al menu **Protezione > Relazioni > Relazioni: Velocità di trasferimento ultimo mese** e utilizzare il **Filtro** per visualizzare solo i dati dei volumi.

- **Dimensione totale del trasferimento**

Visualizza la dimensione totale del volume trasferito 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 visualizzazione **Relazione: MetroCluster**, vedere ["Monitoraggio delle configurazioni MetroCluster"](#) .
- Per informazioni sulla visualizzazione **Relazione: Stato del trasferimento dell'ultimo mese**, vedere ["Relazione: Visualizzazione dello stato del trasferimento dell'ultimo mese"](#) .
- Per informazioni sulla visualizzazione **Relazione: Tutte le relazioni**, vedere ["Relazione: Visualizzazione del tasso di trasferimento dell'ultimo mese"](#)

Genera report personalizzati

Reporting del gestore unificato

Active IQ Unified Manager (in precedenza OnCommand Unified Manager) offre la possibilità di visualizzare, personalizzare, scaricare e pianificare report per i sistemi di archiviazione ONTAP . I report possono fornire dettagli sulla capacità del sistema di archiviazione, sullo stato di salute, sulle prestazioni, sulla sicurezza e sulle relazioni di protezione.

La nuova funzionalità di reporting e pianificazione di Unified Manager introdotta in Active IQ Unified Manager 9.6 sostituisce il precedente motore di reporting che è stato ritirato nella versione 9.5 di Unified Manager.

La reportistica fornisce diverse visualizzazioni della rete, offrendo informazioni fruibili su capacità, integrità, prestazioni, sicurezza e dati di protezione. È possibile personalizzare le visualizzazioni mostrando, nascondendo e riorganizzando le colonne, filtrando i dati, ordinando i dati e cercando i risultati. È possibile salvare le visualizzazioni personalizzate per riutilizzarle, scaricarle come report e programmarle come report ricorrenti da distribuire tramite e-mail.

È possibile scaricare le visualizzazioni in formato Microsoft® Excel e personalizzarle. È possibile utilizzare le funzionalità avanzate di Excel, come ordinamenti complessi, filtri a livelli, tabelle pivot e grafici. Una volta ottenuto il report Excel desiderato, 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 su integrità, sicurezza e prestazioni da Unified Manager utilizzando questi metodi aggiuntivi:

- Utilizzo di Open Database Connectivity (ODBC) e degli strumenti ODBC per accedere direttamente al database per le informazioni sul cluster
- Esecuzione delle API REST di Unified Manager per restituire le informazioni che ti interessa rivedere

A partire da questa versione di Active IQ Unified Manager, sono stati apportati i seguenti miglioramenti ai report:

- Viene inviata un'e-mail per un report in base alla pianificazione configurata. Anche quando generi un report su richiesta, riceverai un'e-mail.
- Il nome del file del report e i metadati del report includono il nome host da cui è stato generato il report. Anche se qualcuno modifica il nome del file, grazie a questo miglioramento è comunque possibile identificare il nome host da cui è stato generato il report.

Punti di accesso per la generazione di report

In Unified Manager puoi raccogliere informazioni sui tuoi cluster per creare report dall'interfaccia utente, dalle query del database MySQL e dalle API REST.

In queste sezioni vengono descritte le funzionalità di reporting e pianificazione di Unified Manager tramite l'interfaccia utente.

Esistono tre modi per accedere alle funzionalità di reporting fornite da Unified Manager:

- Estrazione dei dati direttamente dalle pagine dell'inventario nell'interfaccia utente.

- Utilizzo di Open Database Connectivity (ODBC) e degli strumenti ODBC per accedere a tutti gli oggetti disponibili.
- Esecuzione delle API REST di Unified Manager per restituire le informazioni che si desidera esaminare.

In queste sezioni vengono descritte le funzionalità di reporting e pianificazione di Unified Manager tramite l'interfaccia utente.

Database Unified Manager accessibili per report personalizzati

Unified Manager utilizza un database MySQL per archiviare i dati dei cluster monitorati. I dati vengono conservati in vari schemi nel database MySQL.

Sono disponibili tutti i dati delle tabelle dai seguenti database:

Banca dati	Descrizione
modello_netapp	Dati sugli oggetti sui controller ONTAP .
netapp_model_view	Dati sugli oggetti sui controller ONTAP , adatti all'utilizzo da parte degli strumenti di reportistica.
prestazioni netapp	Contatori delle prestazioni specifici del cluster.
ocum	Dati e informazioni dell'applicazione Unified Manager per supportare il filtraggio dell'interfaccia utente, l'ordinamento e il calcolo di alcuni campi derivati.
ocum_report	Dati per la configurazione dell'inventario e informazioni relative alla capacità.
ocum_report_birt	Visualizzazioni per la configurazione dell'inventario e dati relativi alla capacità, adatte all'utilizzo di strumenti di reportistica.
opm	Impostazioni di configurazione delle prestazioni e informazioni sulla soglia.
monitor di scala	Dati sui problemi di prestazioni e integrità dell'applicazione Unified Manager.
modello_vmware	Dati degli oggetti VMware per datastore ospitati su storage NetApp .
vmware_model_view	Visualizzazioni per dati di oggetti VMware per datastore ospitati su storage NetApp , adatte all'utilizzo tramite strumenti di reportistica.
prestazioni vmware	Dati del contatore delle prestazioni VMware per gli archivi dati ospitati sullo storage NetApp .

Un utente che esegue report, ovvero un utente del database con il ruolo di schema del report, è in grado di accedere ai dati in queste tabelle. Questo utente ha accesso in sola lettura ai report e ad altre visualizzazioni del database direttamente dal database Unified Manager. Si noti che questo utente non ha l'autorizzazione per accedere ad alcuna tabella contenente dati utente o informazioni sulle credenziali del cluster.

API REST di Unified Manager che possono essere utilizzate per la creazione di report

È possibile utilizzare le API REST per gestire i cluster visualizzando le informazioni su integrità, capacità, prestazioni e sicurezza acquisite da Unified Manager.

Le API REST sono accessibili tramite la pagina web Swagger. È possibile accedere alla pagina web di Swagger per visualizzare la documentazione dell'API REST di Unified Manager, nonché per emettere manualmente una chiamata API. Dall'interfaccia utente Web di Unified Manager, nella barra dei menu, fare clic sul pulsante **Guida** e quindi selezionare **Documentazione API**. Per informazioni sulle API REST di Unified Manager, vedere ["Introduzione alle API REST Active IQ Unified Manager"](#).

Per accedere alle API REST è necessario disporre del ruolo di Operatore, Amministratore di archiviazione o Amministratore dell'applicazione.

Comprendere i report

I report mostrano informazioni dettagliate su storage, rete, qualità del servizio e relazioni di protezione, aiutandoti a identificare e risolvere potenziali problemi prima che si verifichino.

Quando personalizzi una vista, puoi 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. È anche possibile scaricare la visualizzazione in Excel per personalizzarla utilizzando le funzionalità avanzate di Excel, quindi caricare nuovamente il file in Unified Manager. Se pianifichi un report utilizzando quella vista, verrà utilizzato il file Excel caricato per creare report efficaci che potrai condividere.

È possibile gestire tutti i report pianificati dalla pagina Pianificazioni report.



Per gestire i report è necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

È possibile scaricare i report come file CSV (valori separati da virgole), Excel o PDF.

Comprendere la relazione tra vista e report

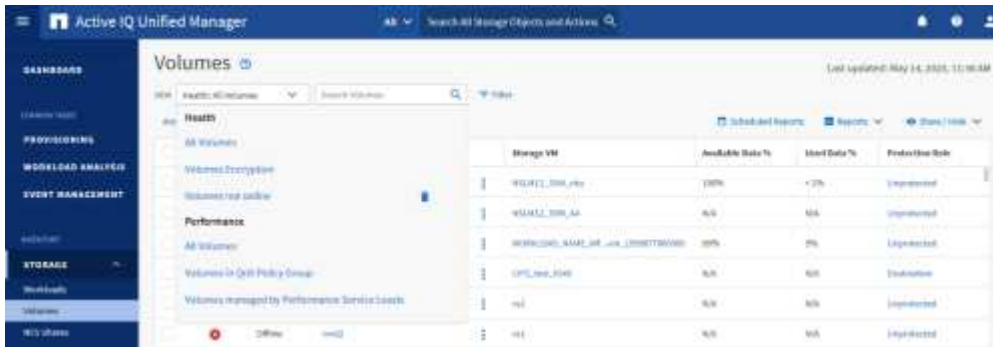
Le visualizzazioni e le pagine di inventario diventano report quando vengono scaricate o pianificate.

È possibile personalizzare e salvare le visualizzazioni e le pagine di inventario per riutilizzarle. Quasi tutto ciò che puoi visualizzare in Unified Manager può essere salvato, riutilizzato, personalizzato, pianificato e condiviso come report.

Nel menu a discesa delle visualizzazioni, gli elementi contrassegnati dall'icona Elimina sono visualizzazioni personalizzate esistenti create da te o da un altro utente. Gli elementi senza icona sono visualizzazioni predefinite fornite con Unified Manager. Le viste predefinite non possono essere modificate o eliminate.



- Se si elimina una visualizzazione personalizzata dall'elenco, verranno eliminati anche tutti i file Excel o i report pianificati che utilizzano tale visualizzazione.
- Se modifichi una visualizzazione personalizzata, i report che utilizzano tale visualizzazione rifletteranno la modifica la prossima volta che il report verrà generato e inviato tramite e-mail in base alla pianificazione del report. Quando si modificano le visualizzazioni, assicurarsi che le modifiche siano compatibili con tutte le personalizzazioni di Excel associate utilizzate per i report. Se necessario, è possibile aggiornare il file Excel scaricandolo, apportando le modifiche necessarie e caricandolo come nuova personalizzazione di Excel per la visualizzazione.



Solo gli utenti con il ruolo di Amministratore applicazione o Amministratore archiviazione possono visualizzare l'icona di eliminazione, modificare o eliminare una visualizzazione oppure 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 che è possibile personalizzare, scaricare e pianificare.

Report Active IQ Unified Manager

Tipo	Oggetto di archiviazione o di rete
Capacità	Cluster
	Aggregati
	Volumi
	Qtrees

Tipo	Oggetto di archiviazione o di rete
Salute	Cluster Nodi Aggregati VM di archiviazione Volumi Azioni SMB/CIFS Azioni NFS
Prestazione	Cluster Nodi Aggregati VM di archiviazione Volumi LUN Spazi dei nomi NVMe Interfacce di rete (LIF) porti
Qualità del servizio	Gruppi di policy QoS tradizionali Gruppi di policy QoS adattive Gruppi di policy del livello di servizio delle prestazioni
Relazioni di protezione del volume (disponibili nella pagina Volumi)	Tutte le relazioni Stato del trasferimento dell'ultimo mese Tasso di trasferimento dell'ultimo mese
Sicurezza	VM di archiviazione Cluster

Limitazioni alla segnalazione

Esistono alcune limitazioni relative alla nuova funzionalità di reporting Active IQ Unified Manager di cui dovresti essere a conoscenza.

Report esistenti dalle versioni precedenti di Unified Manager

È possibile modificare la pianificazione e i destinatari solo per i report esistenti creati e importati (come file .rptdesign) in Unified Manager 9.5 e versioni precedenti. Se hai personalizzato uno qualsiasi dei report standard forniti con Unified Manager 9.5 o versioni precedenti, questi report personalizzati non vengono importati nel nuovo strumento di reporting.

Se è necessario modificare report esistenti importati da file .rptdesign, eseguire una delle seguenti operazioni e rimuovere il report importato:

- creare una nuova vista e pianificare un report da quella vista (preferito)
- passa il mouse sopra il report, copia il codice SQL ed estrai i dati utilizzando uno strumento esterno

Le visualizzazioni predefinite possono essere generate come report senza bisogno di alcuna personalizzazione. È possibile utilizzare la nuova soluzione di reporting per ricreare qualsiasi report personalizzato.

Relazione tra pianificazione e report

È possibile creare numerose pianificazioni diverse con qualsiasi combinazione di destinatari per ogni report salvato. Tuttavia, non è possibile riutilizzare la pianificazione per più report.

Segnala la protezione

Qualsiasi utente con le autorizzazioni appropriate può modificare o eliminare i report. Non è possibile impedire ad altri utenti di rimuovere o modificare visualizzazioni o pianificazioni salvate.

resoconti degli eventi

Sebbene sia possibile personalizzare la visualizzazione degli eventi e scaricare il report risultante in formato CSV, non è possibile pianificare la generazione e la distribuzione di report di eventi ricorrenti.

Segnala allegati

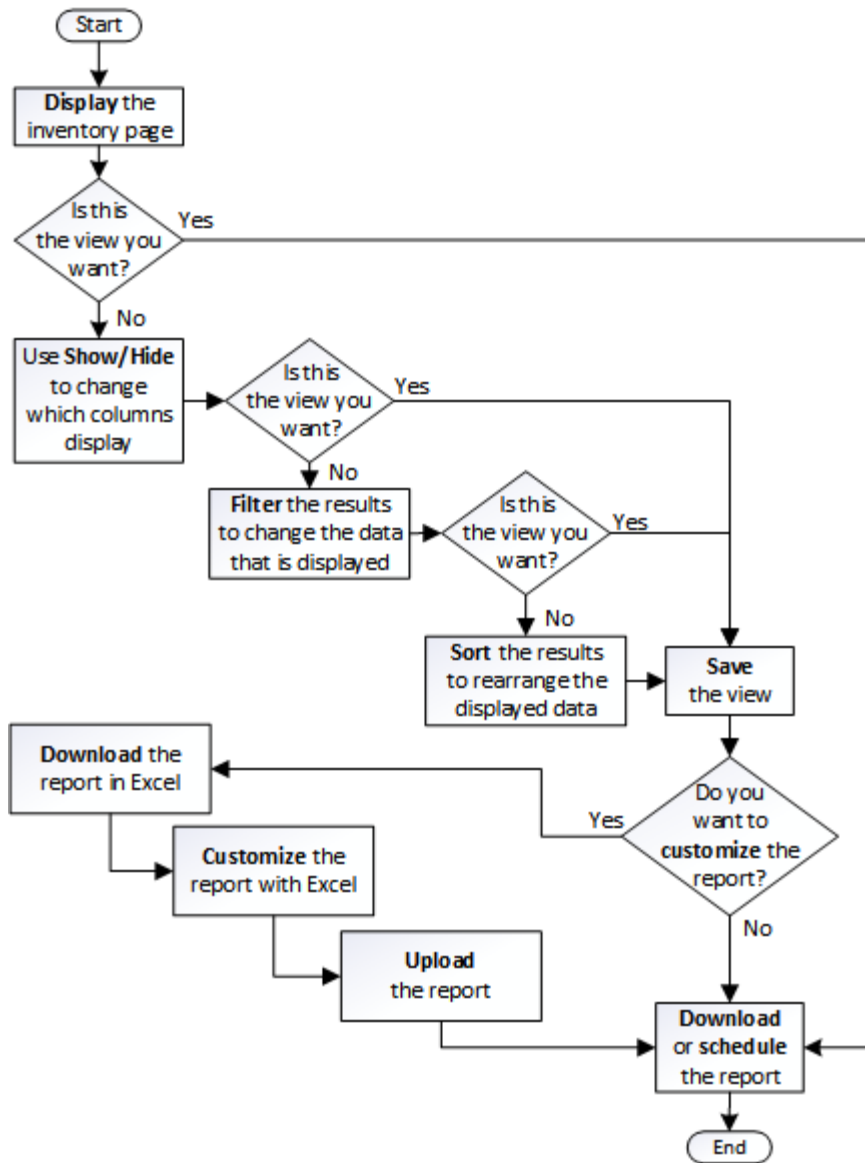
I report non possono essere inviati nel corpo di un'e-mail. I report vengono invece inviati solo come allegati PDF, Excel o CSV.

Lavorare con i report

Scopri come trovare e personalizzare le visualizzazioni delle pagine dell'inventario in report pianificati condivisibili.

Flusso di lavoro del report

Albero decisionale che descrive il flusso di lavoro del report.



Avvio rapido della segnalazione

Crea un report personalizzato di esempio per provare a esplorare le viste e pianificare i report. Questo report di avvio rapido individua un elenco di volumi che potresti voler spostare nel livello cloud perché contengono una discreta quantità di dati inattivi (freddi). Aprirai la vista Prestazioni: Tutti i volumi, personalizzerai la vista utilizzando filtri e colonne, salverai la vista personalizzata come report e programmerai la condivisione del report una volta alla settimana.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato gli aggregati FabricPool e disporre di volumi su tali aggregati.

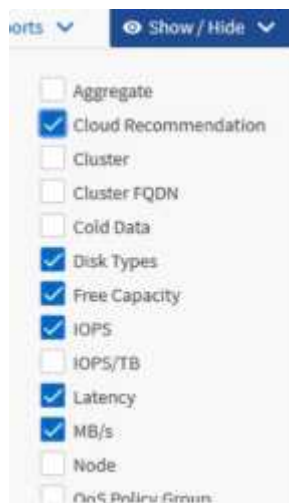
Seguire i passaggi sottostanti per:

- Apri la vista predefinita

- Personalizza le colonne filtrando e ordinando i dati
- Salva la vista
- Pianifica la generazione di un report per la vista personalizzata

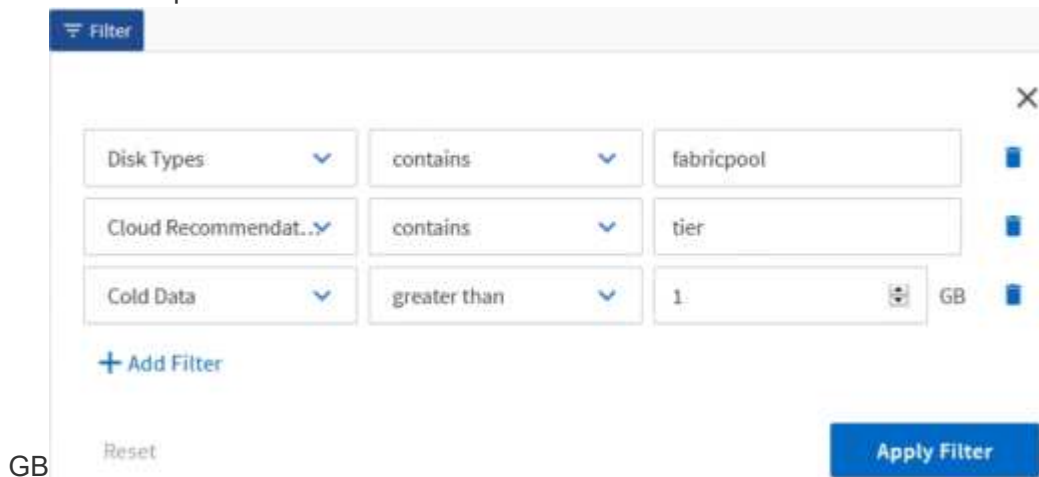
Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Prestazioni > Tutti i volumi**.
3. Fare clic su **Mostra/Nascondi** per assicurarsi che la colonna “Tipi di disco” venga visualizzata nella vista.



Aggiungi o rimuovi altre colonne per creare una vista contenente i campi importanti per il tuo report.

4. Trascina la colonna “Tipi di disco” accanto alla colonna “Raccomandazione cloud”.
5. Fare clic sull'icona del filtro per aggiungere i seguenti tre filtri, quindi fare clic su **Applica filtro**:
 - I tipi di disco contengono FabricPool
 - La raccomandazione cloud contiene il livello
 - Dati freddi superiori a 10



Si noti che ogni filtro è unito tramite un AND logico, in modo che tutti i volumi restituiti debbano soddisfare tutti i criteri. Puoi aggiungere un massimo di cinque filtri.

6. Fare clic sulla parte superiore della colonna Cold Data per ordinare i risultati in modo che i volumi con il

maggior numero di dati cold vengano visualizzati nella parte superiore della vista.

- Quando la vista è personalizzata, il nome della vista è Vista non salvata. Assegnare alla vista un nome che rifletta ciò che la vista stessa mostra, ad esempio “I volumi modificano la politica di tiering”. Al termine, fare clic sul segno di spunta o premere **Invio** per salvare la vista con il nuovo nome.

Volumes - Performance / Vols change tiering policy ⓘ

Last updated: Feb 8, 2019, 12:26 PM ⓘ

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy 🔍 Search Volumes ⓘ

Assign Performance Threshold Policy

Clear Performance Threshold Policy

Scheduled Reports

Reports ▾

Show / Hide ▾

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagntsdzt	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

- Scarica il report come file **CSV**, **Excel** o **PDF** per visualizzare il risultato prima di pianificarlo o condividerlo.

Aprire il file con un'applicazione installata, come Microsoft Excel (CSV o Excel) o Adobe Acrobat (PDF), oppure salvare il file.



È possibile personalizzare ulteriormente il report utilizzando filtri complessi, ordinamenti, tabelle pivot o grafici scaricando la vista come file Excel. Dopo aver aperto il file in Excel, utilizza le funzionalità avanzate per personalizzare il report. Una volta soddisfatti, caricate 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 tramite Excel, vedere *Esempi di report Microsoft Excel*.

- Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario. Nell'elenco vengono visualizzati tutti i report pianificati relativi all'oggetto, in questo caso i volumi.

Assign Performance Threshold Policy

Clear Performance Threshold Policy

Scheduled Reports

Volumes - Scheduled Reports

[View all Scheduled Reports](#)

Add Schedule

Schedule Name	View	Recipients	Frequency	Format	
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV	

- Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
- Inserisci un nome per il report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail 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 Capa	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				

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	kjagnfsdst	Snapshot	28.01	121.32	150	ocum-mo	ocum-mo-01-02	aggr5_vs
Ok	nfs_vol4	Snapshot	379.64	2676.57	3072	ocum-mo	ocum-mo-01-02	aggr4

In base ai risultati mostrati nel report, potresti voler utilizzare ONTAP System Manager o ONTAP CLI per modificare la policy di suddivisione in livelli in "auto" o "all" per determinati volumi, in modo da trasferire più dati inattivi al livello cloud.

Cerca un report programmato

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 **Gestione archiviazione > Pianificazioni report**.
2. Utilizzare il campo di testo **Cerca report pianificati**.

Per trovare i resoconti di ...	Tentativo ...
Nome della pianificazione	Digitare parte del nome della pianificazione del report.
Visualizza nome	Digitare parte del nome della vista del report. Nell'elenco delle visualizzazioni vengono visualizzate le visualizzazioni predefinite e personalizzate.
Destinatario	Digita parte dell'indirizzo email.
Tipo di file	Digita "PDF", "CSV" o "XLSX".

3. È possibile fare clic su un'intestazione di colonna per ordinare i report in ordine crescente o decrescente in base a quella colonna, ad esempio in base al nome della pianificazione o al formato.

Personalizza i report

Esistono molti modi per personalizzare le visualizzazioni in modo da creare un report contenente tutte le informazioni necessarie per gestire i cluster ONTAP .

Inizia con una pagina di inventario predefinita o una vista personalizzata, quindi personalizzala 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 visualizzazione in Excel per personalizzarla utilizzando funzionalità avanzate. Al termine, carica il file Excel personalizzato. Se si pianifica un report utilizzando tale visualizzazione, il file Excel personalizzato viene utilizzato per creare report affidabili che è possibile condividere.

Per ulteriori informazioni sulla personalizzazione dei report tramite Excel, vedere *Esempi di report Microsoft Excel*.



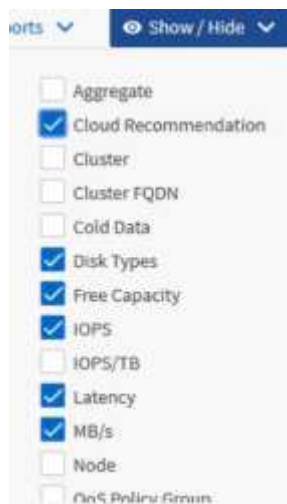
Per gestire i report è necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Personalizza le colonne

Utilizzare **Mostra/Nascondi** per scegliere le colonne che si desidera utilizzare nel report. Trascina le colonne nella pagina dell'inventario per riorganizzarle.

Passi

1. Fare clic su **Mostra/Nascondi** per aggiungere o rimuovere colonne.



2. Nella pagina dell'inventario, trascina le colonne per riorganizzarle nell'ordine desiderato nel report.
3. Assegna un nome alla vista non salvata per salvare le modifiche.

Filtra i dati

Filtra i dati per assicurarti che i risultati corrispondano ai requisiti del tuo report. Il filtraggio consente di visualizzare solo i dati di proprio interesse.

Passi

1. Fare clic sull'icona del filtro per aggiungere filtri e focalizzare i risultati che si desidera visualizzare, quindi fare clic su **Applica filtro**.

The screenshot shows a 'Filter' panel with a close button (X) in the top right. It contains three filter rules, each with a dropdown menu for the field, a dropdown for the operator, and a text input for the value. The first rule is 'Disk Types' contains 'fabricpool'. The second rule is 'Cloud Recommendation' contains 'tier'. The third rule is 'Cold Data' greater than '1' GB. Below the rules is a '+ Add Filter' button. At the bottom are 'Reset' and 'Apply Filter' buttons.

2. Assegna un nome alla vista non salvata per salvare le modifiche.

Ordina i 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.

Passi

1. Fare clic sulla parte superiore di una colonna per ordinare i risultati in modo che le informazioni più importanti vengano visualizzate nella parte superiore della vista.
2. Assegna un nome alla vista non salvata per salvare le modifiche.

Utilizzare la ricerca per perfezionare la visualizzazione

Dopo aver ottenuto la visualizzazione desiderata, puoi perfezionare ulteriormente i risultati utilizzando il campo Cerca per concentrarti sui risultati che desideri includere nel report.

Passi

1. Apri la visualizzazione personalizzata o predefinita che desideri utilizzare come base per il tuo report.
2. Digita nel campo Cerca per restringere i dati elencati nella vista. È possibile immettere dati parziali in una qualsiasi delle colonne visualizzate. Ad esempio, se si desidera cercare nodi che includono "US_East" nel nome, è possibile restringere l'elenco completo dei nodi.

I risultati della ricerca vengono salvati nella vista personalizzata e utilizzati nel report pianificato risultante.

3. Assegna un nome alla vista non salvata per salvare le modifiche.

Utilizza Excel per personalizzare il tuo report

Dopo aver salvato la visualizzazione, è possibile scaricarla in formato cartella di lavoro Excel (.xlsx). Quando apri il file Excel, puoi utilizzare le funzionalità avanzate di Excel per personalizzare il tuo report.

Prima di iniziare

È possibile caricare solo un file di cartella di lavoro Excel con estensione .xlsx.

Ad esempio, alcune funzionalità avanzate di Excel che puoi utilizzare nel tuo report includono:

- Ordinamento multicolonna
- Filtraggio complesso
- Tabelle pivot
- Grafici



- Il file Excel scaricato utilizza il nome file predefinito per la visualizzazione, 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 di file di health-volumes-05-May-2020-19-18-00.xlsx se salvati in quel giorno e a quella ora.
- È possibile aggiungere fogli al file Excel, ma non modificare quelli esistenti.
 - Non modificare i fogli, i dati e le informazioni esistenti. Copia invece i dati in una nuova pagina che hai creato.
 - Un'eccezione alla regola di cui sopra è che è possibile creare formule nella pagina "dati". Utilizzare le formule della pagina dati per creare grafici su nuove pagine.
 - Non assegnare un nome a un nuovo foglio di dati o informazioni.
- Se esiste un file Excel personalizzato, accanto alla voce di menu **Report > Carica Excel** è presente un segno di spunta. Quando si scarica il file Excel, viene utilizzata la versione con



Passi

1. Apri la vista predefinita, personalizzata o salvata che desideri utilizzare come base per il tuo report.
2. Selezionare **Report > Scarica Excel**.
3. Salva 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 oppure, se lavori in un'altra posizione, salva il file nella posizione originale utilizzando il nome file originale prima di caricarlo.
5. Personalizza il file utilizzando le funzionalità di Excel, come ordinamenti complessi, filtri a livelli, tabelle pivot o grafici. Per ulteriori informazioni, consultare la documentazione di Microsoft® Excel.
6. Seleziona **Report > Carica Excel** e seleziona il file che hai modificato. Il file scaricato più di recente viene caricato dalla stessa posizione del file.

7. Inviati un report di prova utilizzando la funzione **Report pianificati**.

Scarica i report

È possibile scaricare i report e salvare i dati su un'unità locale o di rete come file CSV (valori separati da virgole), file Microsoft Excel (.XLSX) o file 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.

Passi

1. Fare clic sul pulsante **Report** per scaricare il report in uno dei seguenti modi:

Scegliere	A...
Scarica CSV	Salvare il report come file CSV (valori separati da virgole).
Scarica PDF	Salvare il report come file .pdf.
Scarica Excel	Salvare il report come file Microsoft Excel (XLSX).

Pianifica i report

Dopo aver creato una vista che desideri riutilizzare e condividere come report, puoi pianificarla utilizzando Active IQ Unified Manager. È possibile gestire i report programmati, modificando i destinatari e la frequenza di distribuzione per ogni pianificazione del report.

In Unified Manager è possibile pianificare la maggior parte delle visualizzazioni o delle pagine di inventario. Le eccezioni sono gli eventi, ovvero report che è possibile scaricare come file CSV, ma non è possibile pianificare eventi per la rigenerazione e la condivisione. Non è inoltre possibile scaricare o pianificare i dashboard, i preferiti o le pagine di configurazione.

A partire da Active IQ Unified Manager 9.8, è possibile scaricare le visualizzazioni in formato Microsoft® Excel e personalizzarle. È possibile utilizzare funzionalità avanzate di Excel, quali ordinamenti complessi, filtri a livelli, tabelle pivot e grafici. Una volta ottenuto il report Excel desiderato, è possibile caricare il file Excel per utilizzarlo ogni volta che il report viene pianificato e condiviso.

È possibile programmare le viste integrate o quelle personalizzate. Puoi scegliere il tipo di file da inviare: CSV, PDF o XSLX. Quando pianifichi un report per la prima volta, puoi scaricarlo e impostarti come unico destinatario a visualizzarlo, così come lo vedranno i tuoi destinatari.

Pianifica un rapporto

Dopo aver creato una vista o un file Excel di cui si desidera pianificare la generazione e la distribuzione regolari, è possibile pianificare il report.

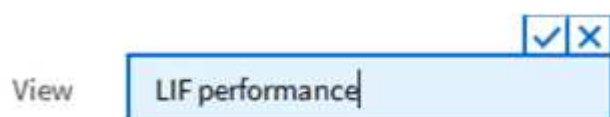
Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato le impostazioni del server SMTP nella pagina **Generale > Notifiche** affinché il motore di reporting possa inviare report come allegati e-mail all'elenco dei destinatari dal server Unified Manager.
- Il server di posta elettronica deve essere configurato per consentire l'invio di allegati con le email generate.

Per testare e pianificare la generazione di un report per una vista, attenersi alla seguente procedura. Seleziona o personalizza la visualizzazione che desideri utilizzare. La seguente procedura utilizza una vista di rete che mostra le prestazioni delle interfacce di rete, ma è possibile utilizzare qualsiasi vista si desideri.

Passi

1. Apri la tua visuale. In questo esempio viene utilizzata la visualizzazione di rete predefinita che mostra le prestazioni LIF. Nel riquadro di navigazione a sinistra, fare clic su **Rete > Interfacce di rete**.
2. Personalizza la visualizzazione in base alle tue esigenze utilizzando le funzionalità integrate di Unified Manager.
3. Dopo aver personalizzato la vista, puoi specificare un nome univoco nel campo **Visualizzazione** e fare clic sul segno di spunta per salvarlo.



4. È possibile utilizzare le funzionalità avanzate di Microsoft® Excel per personalizzare il report. Per i dettagli, vedere ["Utilizzo di Excel per personalizzare il report"](#).
5. Per visualizzare l'output prima di pianificarlo o condividerlo:

Opzione	Descrizione
Se hai utilizzato Excel per personalizzare il report	Visualizza il file Excel scaricato esistente.
Se non hai utilizzato Excel per personalizzare il report	Scarica il report come file CSV , PDF o XLSX .

Aprire il file con un'applicazione installata, come Microsoft Excel (CSV/XSLX) o Adobe Acrobat (PDF).

6. Se sei soddisfatto del report, clicca su **Report pianificati**.
7. Nella pagina Pianificazioni report, fare clic su **Aggiungi pianificazione**.
8. Accetta il nome predefinito, che è una combinazione del nome della vista e della frequenza, oppure personalizza il **nome della pianificazione**.
9. Per testare il report pianificato per la prima volta, aggiungi solo te stesso come **destinatario**. Una volta soddisfatti, aggiungere gli indirizzi email di tutti i destinatari del report.
10. Specificare la frequenza con cui il report verrà generato e inviato ai destinatari. Puoi scegliere **Giornaliero**, **Settimanale** o **Mensile**.
11. Selezionare il formato, **PDF**, **CSV** o **XSLX**.



Per i report in cui hai utilizzato Excel per personalizzare il contenuto, seleziona sempre **XSLX**.

12. Fare clic sul segno di spunta (✓) per salvare la pianificazione del report.

LIFs - Scheduled Reports [View all Scheduled Reports](#)

[Add Schedule](#)

Schedule Name	View	Recipients	Frequency	Format
Weekly / LIF performar	Performance / LIF pe ▼	test@inetapp.com	Weekly ▼ Thursda ▼ 4:30 PM ▼	PDF ▼

✓ ✕

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza pianificata.

Pianifica i report .rptdesign importati

È possibile pianificare report esistenti creati e importati in una versione precedente di Unified Manager.

Per pianificare i report importati è necessario quanto segue:

- report di file .rptdesign progettati da BIRT importati in una versione precedente di Unified Manager
- applicabile durante l'aggiornamento a Unified Manager 9.6 GA o versione successiva

Dopo l'aggiornamento a Unified Manager 9.6 GA o versione successiva, la pagina Pianificazioni report elenca i report importati. È possibile modificare la pianificazione di questi report specificando gli indirizzi e-mail dei destinatari, la frequenza e il formato (PDF o CSV). In caso contrario, questi report non potranno essere modificati o visualizzati nell'interfaccia utente di Unified Manager.

Passi

1. Aprire la pagina Pianificazioni report. Se hai importato dei report, verrà visualizzato un messaggio.
2. Fare clic sul nome **Visualizza** per visualizzare la query SQL utilizzata per generare il report.

**Imported Report**

This report is generated using following database query:

```
SELECT c.name AS 'Cluster', m.name AS 'SVM', v.name AS 'Volume', s.name AS 'Share',
s.path AS 'Path', q.name AS 'Qtree', s.shareProperties AS 'Properties', a.userOrGroup
AS 'User', a.permission AS 'Permission' FROM ocum_report.cifsshare s JOIN
ocum_report.cifsshareacl a ON s.id = a.cifsShareId JOIN ocum_report.cluster c ON
s.clusterId = c.id JOIN ocum_report.svm m ON s.svmId = m.id JOIN
ocum_report.volume v ON s.volumeId = v.id JOIN ocum_report.qtree q ON s.qtreeId =
q.id
```

3. Clicca sull'icona "Altro"  , fare clic su **Modifica**, definire i dettagli della pianificazione del report e salvare il report.



Puoi anche eliminare eventuali segnalazioni indesiderate dall'icona Altro  .

Gestire le pianificazioni dei report

Puoi gestire le pianificazioni dei tuoi report dalla pagina Pianificazioni dei report. È possibile visualizzare, modificare o eliminare le pianificazioni esistenti.



Prima di iniziare

Non è possibile pianificare nuovi report dalla pagina Pianificazioni report. È possibile aggiungere report pianificati solo dalle pagine dell'inventario degli oggetti.

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Pianificazioni report**.
2. Nella pagina Pianificazioni dei report:

Se lo desidera...	Poi...
Visualizza una pianificazione esistente	Scorrere l'elenco dei report esistenti utilizzando le barre di scorrimento e i controlli della pagina.

Se lo desidera...	Poi...
Modifica una pianificazione esistente	- Clicca sull'icona "Altro"  per la pianificazione che desideri utilizzare. - Fare clic su Modifica. - Apportare le modifiche necessarie. - Fare clic sul segno di spunta per salvare le modifiche.
Elimina una pianificazione esistente	- Clicca sull'icona "Altro"  per la pianificazione che desideri utilizzare. - Fare clic su Elimina. - Conferma la tua decisione.

Modifica i report pianificati

Dopo aver pianificato i report, è possibile modificarli nella pagina Pianificazioni report.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Pianificazioni report**.

Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



Se si dispone delle autorizzazioni appropriate, è possibile modificare qualsiasi report e la relativa pianificazione nel sistema.

2. Clicca sull'icona "Altro"  per l'orario che vuoi modificare.
3. Fare clic su **Modifica**.
4. È possibile modificare il **Nome pianificazione**, l'elenco **Destinatari**, la **Frequenza** e il **Formato** per la pianificazione del report.
5. Al termine, fai clic sul segno di spunta per salvare le modifiche.

Elimina i report pianificati

Dopo aver pianificato i report, è possibile eliminarli dalla pagina Pianificazioni report.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione > Pianificazioni report**.

Scheduled Reports ?

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



Se si dispone delle autorizzazioni appropriate, è possibile rimuovere qualsiasi report e la relativa pianificazione dal sistema.

2. Clicca sull'icona "Altro"  per la pianificazione che vuoi rimuovere.
3. Fare clic su **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 visualizzazione personalizzata dalla pagina dell'inventario, verranno eliminati anche tutti i file Excel personalizzati o i report pianificati che utilizzano tale visualizzazione.

Esempi di report personalizzati

Questi report personalizzati di esempio vengono comunemente utilizzati per aiutarti a identificare potenziali problemi e a rispondere a potenziali problemi prima che si verifichino.

L'elenco dei report in questa sezione non è esaustivo e verrà ampliato 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 Amministratore dell'archiviazione.

Personalizza i report di archiviazione del cluster

I report di esempio sullo storage del cluster in questa sezione sono solo esempi per aiutarti a capire come creare report sulla capacità del cluster per aiutarti a monitorare le risorse del tuo sistema di storage.

Crea un report per visualizzare la capacità in base al modello di cluster

È possibile creare un report per analizzare la capacità di archiviazione e l'utilizzo dei cluster in base al modello del sistema di archiviazione.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata che mostri la capacità in base al modello di cluster, utilizzare i passaggi seguenti, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti i cluster**.
3. Selezionare **Mostra/Nascondi** per rimuovere tutte le colonne, come "Cluster FQDN" e "OS Version", che non si desidera visualizzare nel report.
4. Trascinare le colonne "Capacità grezza totale", "Modello/Famiglia" e le tre colonne aggregate vicino alla colonna "Cluster".
5. Fare clic sulla parte superiore della colonna "Modello/Famiglia" per ordinare i risultati in base al tipo di cluster.
6. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Capacità per modello cluster".
7. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
8. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report** in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
9. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler aggiungere più capacità a determinati cluster o aggiornare i modelli di cluster più vecchi.

Creare un report per identificare i cluster con la maggiore capacità LUN non allocata

È possibile creare un report per individuare i cluster con la maggiore capacità LUN non allocata, superiore a 0,5 TB, per identificare dove è possibile aggiungere ulteriori carichi di lavoro.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata che mostri i cluster con la maggiore capacità LUN non allocata, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti i cluster**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
4. Trascinare la colonna "Capacità LUN non allocata" vicino alla colonna "Coppia HA".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - Capacità LUN non allocata superiore a 0,5 TB
6. Fare clic sulla parte superiore della colonna "Capacità LUN non allocata" per ordinare i risultati in base alla maggiore quantità di capacità LUN non allocata.
7. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Capacità LUN più non allocata" e fare clic sul segno di spunta (✓).
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
10. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere opportuno utilizzare la capacità LUN non allocata del cluster.

Crea un report per visualizzare le coppie HA con la capacità più disponibile

È possibile creare un report per individuare le coppie ad alta disponibilità (HA) con la maggiore capacità di provisioning di nuovi volumi e LUN.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata che mostri 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Cluster**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti i cluster**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
4. Trascinare la colonna "Capacità aggregata inutilizzata" vicino alla colonna "Coppia HA".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - Capacità aggregata inutilizzata maggiore di 0,5 TB

6. Fare clic sulla parte superiore della colonna "Capacità aggregata inutilizzata" per ordinare i risultati in base alla maggiore quantità di capacità aggregata inutilizzata.
7. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Capacità aggregata meno utilizzata" e fare clic sul segno di spunta (✓).
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
10. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler bilanciare le coppie HA in base alla capacità aggregata.

Crea 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 sapere quali nodi aggiornare.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata che mostri i nodi che eseguono versioni precedenti di ONTAP e quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Nodi**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desidera visualizzare nel report.
3. Trascina la colonna "Versione del sistema operativo" vicino alla colonna "Nodo".
4. Fare clic sulla parte superiore della colonna "Versione del sistema operativo" per ordinare i risultati in base alla versione più vecchia di ONTAP.
5. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Nodi per versione ONTAP".
6. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
7. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
8. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere opportuno aggiornare i nodi che eseguono versioni precedenti di ONTAP.

Personalizza i report sulla capacità aggregata

Questi report personalizzati di esempio vengono utilizzati per aiutarti a identificare e rispondere a potenziali problemi correlati alla capacità di archiviazione aggregata.

I report in questa sezione sono solo esempi per aiutarti a capire come creare report sulla capacità aggregata per aiutarti a monitorare le risorse del tuo sistema di archiviazione.

Crea un report per visualizzare gli aggregati che raggiungono la piena capacità

È possibile creare un report per individuare gli aggregati che stanno raggiungendo la piena capacità, in modo da poter aggiungere ulteriore capacità o spostare i carichi di lavoro su altri aggregati.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata che mostri gli aggregati che raggiungono la piena capacità, utilizzare i passaggi seguenti, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti gli aggregati**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
4. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - Giorni per completare meno di 45 giorni
5. Fare clic sulla parte superiore della colonna "Giorni rimanenti al raggiungimento della piena capacità" 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 sta mostrando, ad esempio "Giorni per raggiungere la piena capacità aggregata", e fare clic sul segno di spunta (✓).
7. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
8. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report** in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
9. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler aumentare lo spazio di archiviazione sugli aggregati che raggiungono la piena capacità. Inoltre, potresti voler aumentare la soglia Giorni fino al raggiungimento della capacità completa a un valore superiore ai 7 giorni predefiniti, in modo da ricevere eventi che offrano più tempo per reagire alla scarsità di spazio sugli aggregati.

Crea un report per visualizzare gli aggregati pieni all'80% o più

È possibile creare un report per evidenziare gli aggregati pieni all'80% o più.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata che mostri aggregati pieni all'80% o più, attenersi alla seguente procedura, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti gli aggregati**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
4. Trascinare le colonne "Dati disponibili %" e "Dati utilizzati %" vicino alla colonna "Aggregato".
5. Fare clic sull'icona del filtro, aggiungere i seguenti filtri e quindi fare clic su **Applica filtro**:
 - La percentuale di dati utilizzati è maggiore dell'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 la vista sta mostrando, ad esempio "Aggregati quasi pieni", e fare clic sul segno di spunta (✓) .
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
10. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler spostare alcuni dati da determinati aggregati.

Crea un report per visualizzare gli aggregati sovraccaricati

È possibile creare un report per analizzare la capacità di archiviazione e l'utilizzo degli aggregati, nonché per visualizzare gli aggregati sovradimensionati.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata che mostri gli aggregati che superano la soglia di impegno eccessivo, attenersi alla seguente procedura, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti gli aggregati**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desidera visualizzare nel report.
4. Trascinare la colonna "Capacità sovraccaricata %" vicino alla colonna "Aggregato".
5. Fare clic sull'icona del filtro, aggiungere i seguenti filtri e quindi fare clic su **Applica filtro**:
 - La capacità sovraccaricata % è maggiore del 100%

6. Fare clic sulla parte superiore della colonna “Capacità sovraccaricata %” per ordinare i risultati in base alla percentuale di capacità.
7. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio “Aggregati sovracommissionati”, e fare clic sul segno di spunta (✓).
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell’inventario.
9. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
10. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler aggiungere ulteriore capacità agli aggregati o spostare alcuni dati da determinati aggregati.

Personalizza i report sulla capacità del volume

Questi report personalizzati di esempio vengono utilizzati per aiutarti a identificare e rispondere a potenziali problemi relativi alla capacità del volume e alle prestazioni.

Crea un report per identificare i volumi prossimi alla piena capacità in cui l'eliminazione automatica degli snapshot è disattivata

È possibile creare un report contenente l'elenco dei volumi che stanno per raggiungere la piena capacità con la funzionalità di eliminazione automatica degli snapshot disattivata. I risultati possono aiutare a identificare i volumi in cui potrebbe essere opportuno configurare l'eliminazione automatica degli snapshot.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Seguire i passaggi seguenti per creare una vista personalizzata che mostri le colonne richieste nell'ordine corretto, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti i volumi**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
4. Trascina e rilascia le colonne “Eliminazione automatica snapshot” e “Giorni mancanti al completamento” vicino alla colonna “Capacità dati disponibile”.
5. Fare clic sull'icona del filtro, aggiungere i due filtri seguenti, quindi fare clic su **Applica filtro**:
 - Giorni mancanti alla scadenza meno di 30 giorni
 - L'eliminazione automatica degli snapshot è disabilitata
6. Fare clic sulla parte superiore della colonna **Giorni rimanenti** in modo che i volumi con il minor numero di giorni rimanenti vengano visualizzati in cima all'elenco.

7. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio “Volumi prossimi alla capacità”.
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler abilitare l'eliminazione automatica degli snapshot sui volumi o trovare un modo per aumentare lo spazio disponibile.

Crea un report per identificare lo spazio utilizzato dai volumi con il thin provisioning disabilitato

Quando un volume non è sottoposto a thin provisioning, occupa l'intero spazio sul disco definito al momento della creazione del volume. L'identificazione dei volumi in cui il thin provisioning è disabilitato aiuta a decidere se abilitare il thin provisioning su determinati volumi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Seguire i passaggi seguenti per creare una vista personalizzata che mostri le colonne richieste nell'ordine corretto, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Capacità > Tutti i volumi**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
4. Trascinare e rilasciare le colonne “Dati utilizzati %” e “Thin Provisioning” vicino alla colonna “Capacità dati disponibile”.
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, **Thin provisioning è No**, quindi fare clic su **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 in cima all'elenco.
7. Salvare la vista con un nome che rifletta ciò che la vista sta mostrando, ad esempio “Volumi senza thin provisioning”.
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report**, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
10. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere opportuno abilitare il thin provisioning su determinati

volumi.

Creare un report per identificare i volumi sugli aggregati FabricPool che dovrebbero spostare i dati al livello cloud

È possibile creare un report contenente l'elenco dei volumi che attualmente risiedono sugli aggregati FabricPool, che hanno una raccomandazione cloud di livello Tier e che contengono una grande quantità di dati inattivi. Questo report può aiutarti a decidere se modificare la politica di suddivisione in livelli per determinati volumi in "auto" o "all" per scaricare più dati inattivi (cold) sul livello cloud.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato gli aggregati FabricPool e disporre di volumi su tali aggregati.

Seguire i passaggi seguenti per creare una vista personalizzata che mostri le colonne richieste nell'ordine corretto, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Prestazioni > Tutti i volumi**.
3. Nel selettore di colonne, assicurati che la colonna "Tipo di disco" sia visualizzata.

Aggiungi o rimuovi altre colonne per creare una visualizzazione importante per il tuo report.

4. Trascina e rilascia la colonna "Tipo di disco" accanto alla colonna "Raccomandazione cloud".
5. Fare clic sull'icona del filtro, aggiungere i seguenti tre filtri, quindi fare clic su **Applica filtro**:
 - Il tipo di disco contiene FabricPool
 - La raccomandazione cloud contiene il livello
 - Dati freddi superiori a 10 GB

Disk Types	contains	fabricpool	
Cloud Recommendation	contains	tier	
Cold Data	greater than	10 GB	

+ Add Filter

Reset Cancel Apply Filter

6. Fare clic sulla parte superiore della colonna Cold Data in modo che i volumi con la maggior parte dei dati cold vengano visualizzati nella parte superiore della vista.

7. Salva la vista con un nome che rifletta ciò che mostra, ad esempio “I volumi modificano la politica di livelli”.

Volumes - Performance / Vols change tiering policy ⓘ

Last updated: Feb 8, 2019, 12:26 PM ↻

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy ▼ 🔍 Search Volumes ≡ 3

Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report			⬇	⚙
Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity		
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB		
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB		

8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
10. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler utilizzare System Manager o ONTAP CLI per modificare la policy di suddivisione in livelli in “auto” o “all” per determinati volumi, in modo da trasferire più dati inattivi al livello cloud.

Personalizza i report sulla capacità di Qtree

Questi report personalizzati di esempio vengono utilizzati per aiutarti a identificare e rispondere a potenziali problemi relativi alla capacità di Qtree.

Crea un report per visualizzare i qtree quasi pieni

È possibile creare un report per analizzare la capacità di archiviazione e l'utilizzo dei qtree e per visualizzare i qtree quasi pieni.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata che mostri i qtree quasi pieni e quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Qtrees**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
3. Trascinare la colonna “Disco utilizzato %” vicino alla colonna “Qtrees”.
4. Fare clic sull'icona del filtro, aggiungere i seguenti filtri e quindi fare clic su **Applica filtro**:

- La percentuale di utilizzo del disco è superiore al 75%
5. Fare clic sulla parte superiore della colonna “Disco utilizzato %” per ordinare i risultati in base alla percentuale di capacità.
 6. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio “Qtrees quasi pieno”, e fare clic sul segno di spunta (✓).
 7. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
 8. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report**, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
 9. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler regolare i limiti rigidi e flessibili del disco (se impostati) oppure bilanciare i dati tra i qtrees.

Personalizza i report di condivisione NFS

È possibile personalizzare i report di condivisione NFS per analizzare le informazioni sulle policy e le regole di esportazione NFS per i volumi sui sistemi di archiviazione. Ad esempio, è possibile personalizzare i report per visualizzare i volumi con percorsi di montaggio inaccessibili e i volumi con i criteri di esportazione predefiniti.

Crea un report per visualizzare i volumi che hanno un percorso di montaggio inaccessibile

È possibile creare un report per individuare i volumi con un percorso di montaggio inaccessibile.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata per i volumi che hanno un percorso di montaggio inaccessibile, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Condivisioni NFS**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desidera visualizzare nel report.
3. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - Il percorso attivo del monte è No
4. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio “Volumi con un percorso di montaggio inaccessibile” e fare clic sul segno di spunta (✓).
5. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
6. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
7. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul

segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler correggere i percorsi di montaggio inaccessibili.

Crea un report per visualizzare i volumi che utilizzano la policy di esportazione predefinita

È possibile creare un report per individuare i volumi che utilizzano la policy di esportazione predefinita.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata per i volumi che utilizzano il criterio di esportazione predefinito, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Condivisioni NFS**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desidera visualizzare nel report.
3. Trascinare la colonna "Criterio di esportazione" vicino alla colonna "Volume".
4. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - La politica di esportazione contiene le impostazioni predefinite
5. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Volumi con una politica di esportazione predefinita" e fare clic sul segno di spunta (✓).
6. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
7. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
8. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler configurare una policy di esportazione personalizzata.

Personalizza i report delle VM di archiviazione

È possibile creare report sulle VM di archiviazione per analizzare le informazioni sui volumi e visualizzare lo stato generale di integrità e la disponibilità dell'archiviazione. Ad esempio, è possibile creare report per visualizzare le SVM che raggiungono il conteggio massimo del volume e per analizzare le SVM arretrate.

Crea un report per visualizzare le VM di archiviazione che raggiungono il limite massimo del volume

È possibile creare un report per individuare le SVM che raggiungono il limite massimo del volume.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata che mostri le VM di archiviazione che stanno raggiungendo il limite massimo del volume, utilizzare i passaggi seguenti, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
3. Trascinare le colonne "Numero volumi" e "Numero massimo di volumi consentiti" vicino alla colonna "VM di archiviazione".
4. Fare clic sulla parte superiore della colonna "Volumi massimi consentiti" per ordinare i risultati in base al numero più alto di volumi.
5. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "SVM che raggiungono i volumi massimi" e fare clic sul segno di spunta (✓).
6. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
7. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report** in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
8. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere opportuno bilanciare i volumi assegnati alle VM di archiviazione o, se possibile, utilizzare ONTAP System Manager per modificare i volumi massimi consentiti.

Crea un report per visualizzare le VM di archiviazione arrestate

È possibile creare un report per visualizzare un elenco di tutte le SVM arrestate.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata che mostri le VM di archiviazione arrestate, attenersi alla seguente procedura e quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Nel menu Visualizza, seleziona **Integrità > Tutte le VM di archiviazione**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desidera visualizzare nel report.
4. Trascinare la colonna "Stato" vicino alla colonna "VM di archiviazione".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - Lo stato è fermo
6. Salvare la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "SVM arrestate" e fare clic sul segno di spunta (✓).

7. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
8. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report** in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
9. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler indagare sul motivo per cui l'SVM è stato arrestato per vedere se è necessario riavviare gli SVM arrestati.

Personalizza i report sulle relazioni di volume

Il report Inventario relazioni volume consente di analizzare i dettagli dell'inventario di storage in un cluster, comprendere il livello di protezione richiesto per i volumi e filtrare i dettagli del volume in base all'origine dell'errore, al modello e alle pianificazioni.

Creare un report per raggruppare le relazioni di volume in base all'origine dell'errore

È possibile creare un report che raggruppa i volumi in base al motivo per cui la relazione non è in uno stato corretto.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata che raggruppi i volumi in base all'origine dell'errore e quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Relazione > Tutte le relazioni**.
3. Selezionare **Mostra/Nascondi** per assicurarsi che le colonne "Stato della relazione" e "Motivo non corretto" vengano visualizzate nella vista.

Aggiungi o rimuovi altre colonne per creare una visualizzazione importante per il tuo report.

4. Trascina le colonne "Salute della relazione" e "Motivo malsano" vicino alla colonna "Stato".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - La salute delle relazioni è pessima
6. Fare clic sulla parte superiore della colonna "Motivo non corretto" per raggruppare le relazioni di volume in base all'origine dell'errore.
7. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Relazioni di volume per errore".
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

Sulla base dei risultati mostrati nel report, è possibile analizzare l'origine e l'impatto di ciascun tipo di errore.

Creare un report per raggruppare le relazioni di volume in base al problema

È possibile creare un report che raggruppi le relazioni di volume in base al problema.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata che raggruppi le relazioni di volume in base al problema, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Relazione > Tutte le relazioni**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.
4. Trascina la colonna "Motivo non salutare" vicino alla colonna "Stato".
5. Fare clic sulla parte superiore della colonna "Motivo non corretto" per raggruppare i volumi in base al problema.
6. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Relazioni tra volumi per problema".
7. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
8. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

Sulla base dei risultati mostrati nel report, è possibile analizzare l'origine e l'impatto di ogni tipo di problema.

Crea un report per visualizzare le tendenze del trasferimento del volume a intervalli di tempo specifici

È possibile creare un report che visualizza le tendenze del trasferimento del volume a intervalli di tempo specifici.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata per i volumi a intervalli di tempo specifici, quindi pianificare la generazione di un report per tale vista, attenersi alla seguente procedura.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Relazione > Stato del trasferimento dell'ultimo mese**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desiderano nel report.

4. Trascinare la colonna Durata del trasferimento vicino alla colonna "Risultato operativo".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - Ora di fine del trasferimento negli ultimi 7 giorni
6. Fare clic sulla parte superiore della colonna "Durata del trasferimento" per ordinare i volumi in base all'intervallo di tempo.
7. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Volumi per durata".
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Inserisci un nome per la pianificazione del report, imposta la frequenza su **Settimanale** e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

Sulla base dei risultati mostrati nel report, è possibile analizzare gli intervalli di tempo di trasferimento.

Crea un report per visualizzare il trasferimento del volume riuscito o non riuscito

È possibile creare un report che visualizza lo stato dei trasferimenti di volume. In questo report è possibile visualizzare sia i trasferimenti di volume riusciti che quelli falliti.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata che mostri quali trasferimenti sono falliti e quali sono riusciti, procedere come segue, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Relazione > Stato del trasferimento dell'ultimo mese**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne che non si desidera visualizzare nel report.
4. Trascinare la colonna "Risultato operazione" vicino alla colonna "Stato".
5. Fare clic sulla parte superiore della colonna "Risultato operazione" per ordinare i volumi in base allo stato.
6. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Volumi per stato di trasferimento".
7. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
8. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile esaminare lo stato del trasferimento.

Crea 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.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata per i trasferimenti di volume in base alle dimensioni del trasferimento, utilizzare i passaggi seguenti, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Relazione > Tasso di trasferimento ultimo mese**.
3. Fare clic sulla parte superiore della colonna "Dimensione totale del trasferimento" per ordinare i trasferimenti di volume in base alla dimensione.
4. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Volumi per dimensione di trasferimento".
5. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
6. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

Sulla base dei risultati mostrati nel report, è possibile analizzare le relazioni di volume in base alle dimensioni del trasferimento.

Crea 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.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per creare una vista personalizzata per i trasferimenti di volume raggruppati per giorno, utilizzare i passaggi seguenti, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Relazione > Tasso di trasferimento ultimo mese**.
3. Fare clic sulla parte superiore della colonna "Giorno" per ordinare i trasferimenti di volume per giorno.
4. Salva la vista con un nome specifico che rifletta ciò che la vista mostra, ad esempio "Trasferimenti di volume per giorno".
5. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
6. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

Sulla base dei risultati mostrati nel report, è possibile analizzare i trasferimenti di volume per giorno.

Personalizza i report sulle prestazioni del volume

Questi report personalizzati di esempio vengono utilizzati per aiutarti a identificare e rispondere a potenziali problemi relativi alle prestazioni del volume.

Crea un report per visualizzare volumi con un'elevata quantità di dati inattivi su un aggregato che non è abilitato per FabricPool

È possibile creare un report per visualizzare volumi con un'elevata quantità di dati inattivi su un aggregato non abilitato per FabricPool . Ciò può aiutarti a identificare i volumi che devono essere spostati in un aggregato FabricPool .

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Utilizzare i passaggi seguenti per creare una vista personalizzata per volumi con un'elevata quantità di dati inattivi su un aggregato non abilitato per FabricPool, quindi pianificare la generazione di un report per tale vista.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Nel menu Visualizza, seleziona **Prestazioni > Tutti i volumi**.
3. Selezionare **Mostra/Nascondi** per assicurarsi che la colonna "Tipo di disco" venga visualizzata nella vista.

Aggiungi o rimuovi altre colonne per creare una visualizzazione importante per il tuo report.

4. Trascinare la colonna "Tipo di disco" vicino alla colonna "Dati inattivi".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro e quindi fare clic su **Applica filtro**:
 - Dati freddi superiori a 100 GB
 - Il tipo di disco contiene SSD
6. Fare clic sulla parte superiore della colonna "Tipo di disco" per ordinare i volumi in base al tipo di disco, in modo che il tipo di disco SSD (FabricPool) sia in basso.
7. Salva la vista con un nome specifico che rifletta ciò che la vista sta mostrando, ad esempio "Volumi dati inattivi non FabricPool".
8. Fare clic sul pulsante **Rapporti pianificati** nella pagina dell'inventario.
9. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

Sulla base dei risultati mostrati nel report, è possibile individuare i volumi che rappresentano buoni candidati per essere trasferiti agli aggregati FabricPool .

Esempi di report di Microsoft Excel

Questi report di esempio di Microsoft Excel hanno lo scopo di presentare 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 su come utilizzare Excel, consultare la documentazione del prodotto.



Per gestire i report è necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Crea un report per mostrare 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 grafico a colonne raggruppate.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per aprire una vista 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, procedere come segue.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Selezionare **Report > Scarica Excel**.



A seconda del browser utilizzato, potrebbe essere necessario fare clic su **OK** per salvare il file.

3. Se necessario, fare clic su **Abilita modifica**.
4. In Excel, apri il file scaricato.
5. Crea un nuovo foglio () dopo il data foglio e chiamalo **Capacità dati totale**.
6. Aggiungere le seguenti colonne al nuovo foglio Capacità dati totale:
 - a. Capacità totale dei dati (GB)
 - b. Capacità impegnata (GB)

- c. Capacità dati utilizzata (GB)
- d. Capacità dati disponibile (GB)

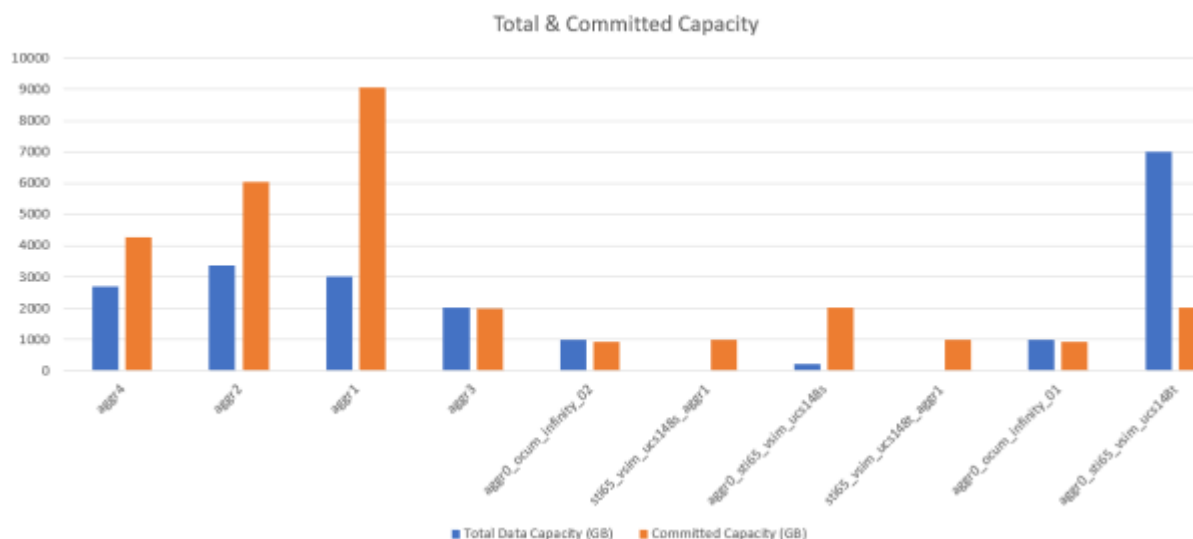
7. Nella prima riga di ogni colonna, immettere la seguente formula, assicurandosi che faccia riferimento al foglio dati (dati!) e che faccia riferimento agli specificatori di colonna e riga corretti per i dati acquisiti (Total Data Capacity estrae i dati dalla colonna E, righe da 2 a 20).

- a. =SOMMA(dati!E\$2:dati!E\$20)
- b. =SOMMA(dati!F\$2:dati!F\$50)
- c. =SOMMA(dati!G\$2:dati!G\$50)
- d. =SOMMA(dati!H\$2:dati!H\$50)

La formula calcola il totale di 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. Nel foglio dati, seleziona le colonne **Capacità dati totale (GB)** e **Capacità impegnata (GB)**.
2. Selezionare **Grafici consigliati** dal menu **Inserisci** e selezionare il grafico **Colonne raggruppate**.
3. Fare clic con il pulsante destro del mouse sul grafico e selezionare **Sposta grafico** per spostare il grafico nella Total Data Capacity foglio.
4. Utilizzando i menu **Design** e **Formato**, disponibili quando il grafico è selezionato, è possibile personalizzare l'aspetto del grafico.
5. Una volta soddisfatti, salvate il file con le modifiche. Non modificare il nome o il percorso del file.



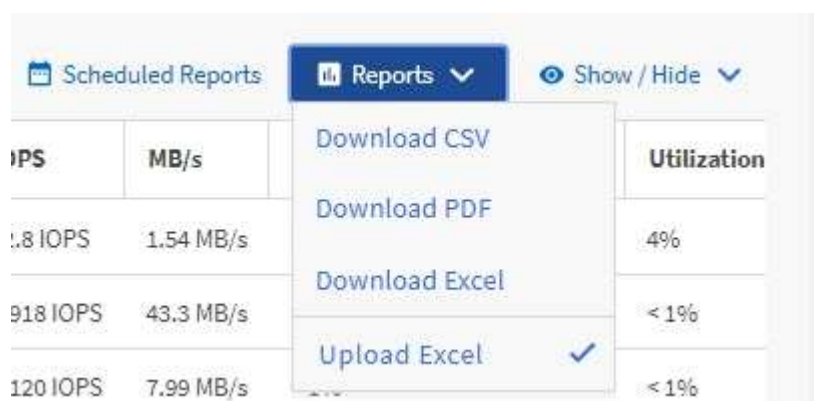
6. In Unified Manager, seleziona **Report > Carica Excel**.



Assicurati di essere nella stessa vista in cui hai scaricato il file Excel.

7. Seleziona il file Excel che hai modificato.
8. Fare clic su **Apri**.
9. Fare clic su **Invia**.

Accanto alla voce di menu **Report > Carica Excel** appare un segno di spunta.



10. Fare clic su **Report pianificati**.

11. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.



Selezionare il formato **XLSX** per il report.

12. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

Sulla base dei risultati mostrati nel report, potresti voler valutare come utilizzare al meglio la capacità disponibile sulla tua rete.

Crea un report per mostrare grafici aggregati della capacità totale rispetto a quella disponibile

È possibile creare un report per analizzare la capacità totale di archiviazione e quella impegnata in un formato grafico Excel.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per aprire una vista Integrità: 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, procedere come segue.

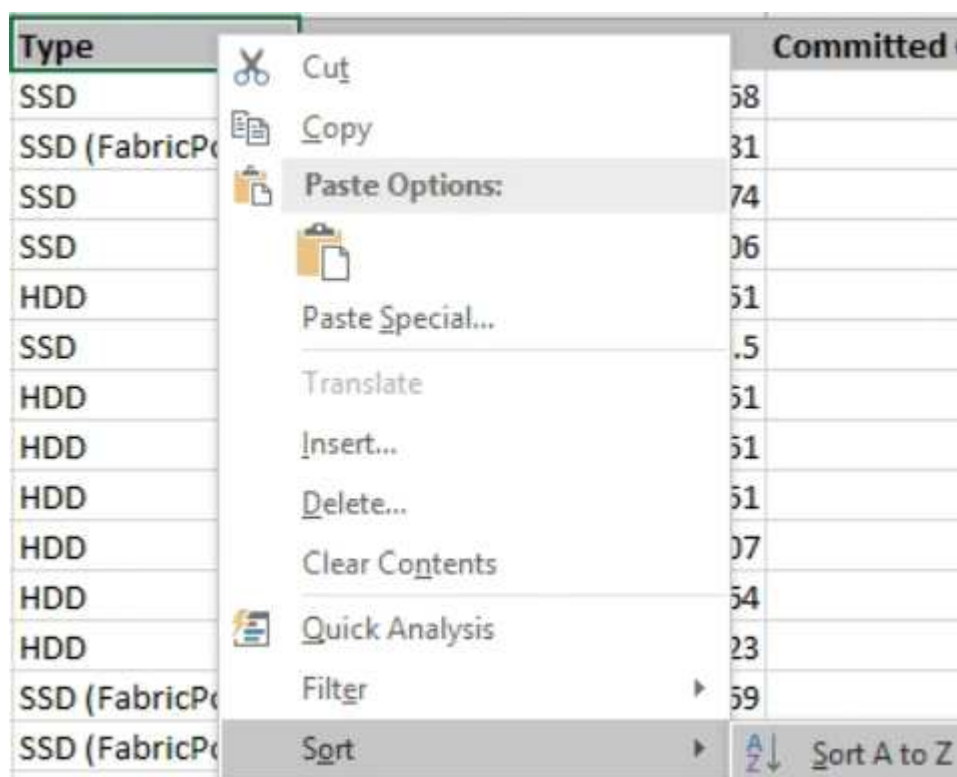
Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Selezionare **Report > Scarica Excel**.



A seconda del browser utilizzato, potrebbe essere necessario fare clic su **OK** per salvare il file.

3. In Excel, apri il file scaricato.
4. Se necessario, fare clic su **Abilita modifica**.
5. Nel foglio dati, fare clic con il pulsante destro del mouse sulla colonna Tipo e selezionare **Ordina > Ordina dalla A alla Z**.



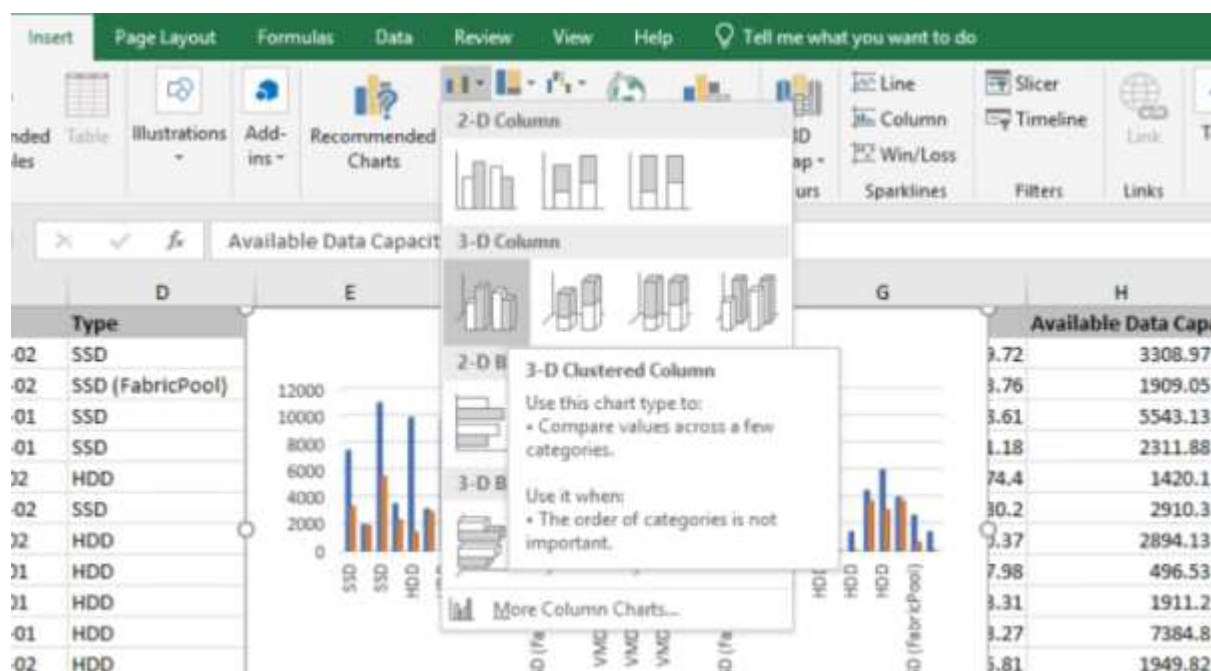
In questo modo i dati verranno organizzati in base al tipo di archiviazione, ad esempio:

- Disco rigido
- Ibrido
- SSD
- SSD (FabricPool)

6. Seleziona il Type, Total Data Capacity, E Available Data Capacity colonne.

7. Nel menu **Inserisci**, seleziona un 3-D column grafico.

Il grafico appare sulla scheda dati.



8. Fare clic con il pulsante destro del mouse sul grafico e selezionare **Sposta grafico**.

9. Selezionare **Nuovo foglio** e rinominare il foglio **Grafici di archiviazione totale**.

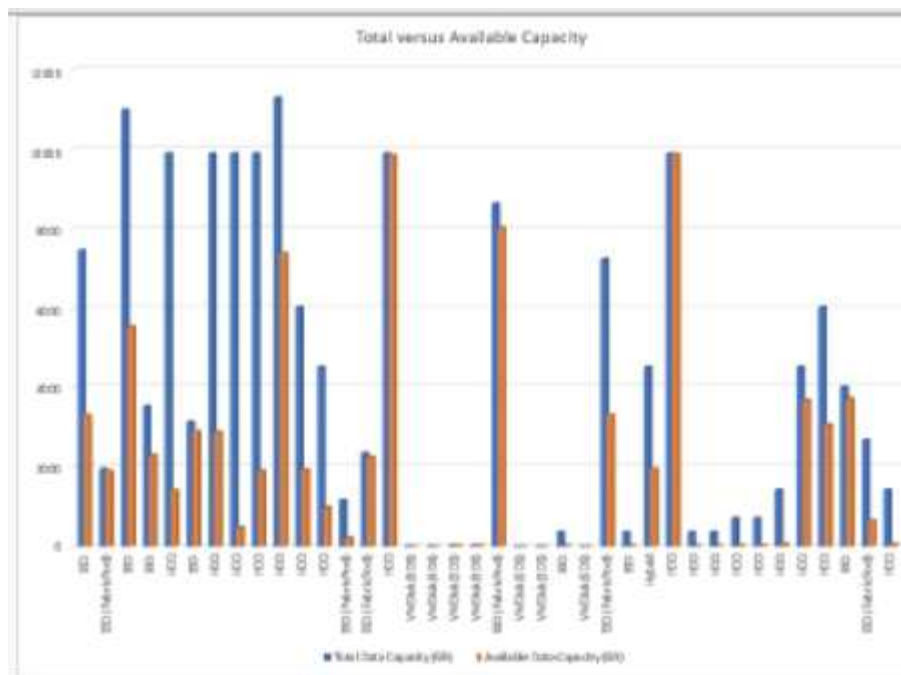


Assicuratevi che il nuovo foglio venga visualizzato dopo le schede informative e quelle tecniche.

10. Assegnare al grafico il titolo **Capacità totale rispetto a capacità disponibile**.

11. Utilizzando i menu **Design** e **Formato**, disponibili quando il grafico è selezionato, è possibile personalizzare l'aspetto del grafico.

12. Una volta soddisfatti, salvate il file con le modifiche. Non modificare il nome o il percorso del file.



13. In Unified Manager, seleziona **Report** > **Carica Excel**.



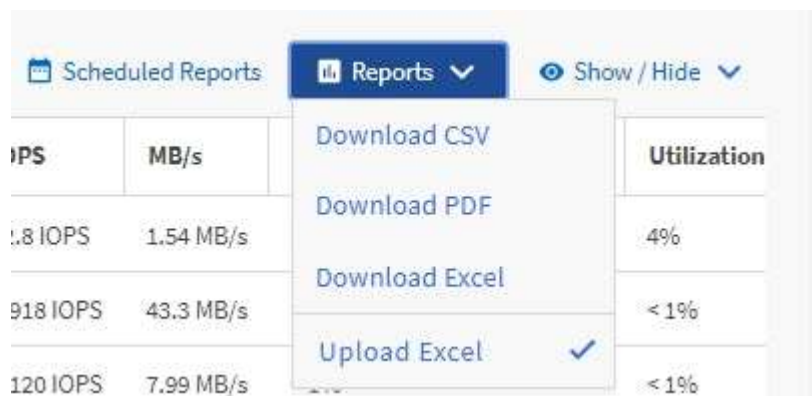
Assicurati di essere nella stessa vista in cui hai scaricato il file Excel.

14. Seleziona il file Excel che hai modificato.

15. Fare clic su **Apri**.

16. Fare clic su **Invia**.

Accanto alla voce di menu **Report** > **Carica Excel** appare un segno di spunta.



17. Fare clic su **Report pianificati**.

18. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report** in modo da poter definire le caratteristiche della pianificazione per il nuovo report.



Selezionare il formato **XLSX** per il report.

19. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler bilanciare il carico sugli aggregati.

Crea un report per visualizzare i grafici della capacità del volume disponibile

È possibile creare un report per analizzare la capacità di volume disponibile in un grafico Excel.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per aprire una vista Integrità: Tutti i volumi, scaricare la vista in Excel, creare un grafico della capacità disponibile, caricare il file Excel personalizzato e pianificare il report finale, procedere come segue.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Volumi**.
2. Selezionare **Report > Scarica Excel**.



A seconda del browser utilizzato, potrebbe essere necessario fare clic su **OK** per salvare il file.

3. Se necessario, fare clic su **Abilita modifica**.
4. In Excel, apri il file scaricato.
5. Sul data foglio, seleziona i dati che vuoi utilizzare nel Volume E Available Data % colonne.
6. Nel menu **Inserisci**, seleziona un 3-D piechart.

Il grafico mostra quali volumi hanno il maggiore spazio disponibile. Il grafico appare sulla scheda dati.



A seconda della configurazione della rete, la selezione di intere colonne o di troppe righe di dati potrebbe rendere illeggibile il grafico a torta. In questo esempio viene utilizzato il grafico a torta 3D, ma è possibile utilizzare qualsiasi tipo di grafico. Utilizza il grafico che meglio visualizza i dati che vuoi acquisire.

7. Assegna al grafico il titolo **Capacità disponibile**.

8. Fare clic con il pulsante destro del mouse sul grafico e selezionare **Sposta grafico**.
9. Selezionare **Nuovo foglio** e rinominare il foglio **Grafici del volume di archiviazione**.



Assicuratevi che il nuovo foglio venga visualizzato dopo le schede informative e quelle tecniche.



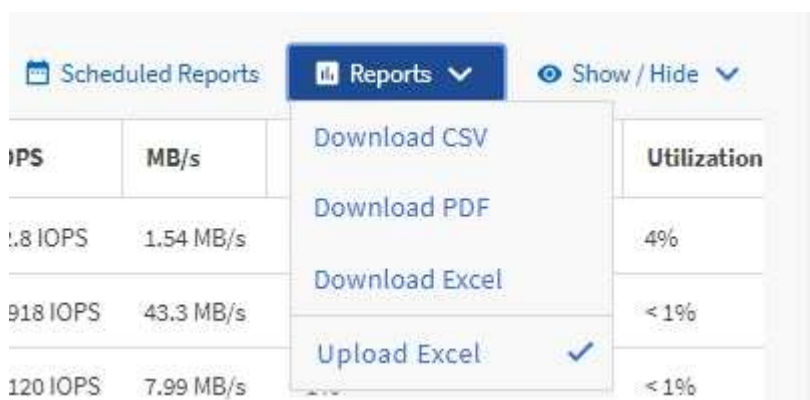
10. Utilizzando i menu **Design** e **Formato**, disponibili quando il grafico è selezionato, è possibile personalizzare l'aspetto del grafico.
11. Una volta soddisfatti, salvate il file con le modifiche.
12. In Unified Manager, seleziona **Report > Carica Excel**.



Assicurati di essere nella stessa vista in cui hai scaricato il file Excel.

13. Seleziona il file Excel che hai modificato.
14. Fare clic su **Apri**.
15. Fare clic su **Invia**.

Accanto alla voce di menu **Report > Carica Excel** appare un segno di spunta.



16. Fare clic su **Report pianificati**.
17. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina **Pianificazioni report** in

modo da poter definire le caratteristiche della pianificazione per il nuovo report.

18. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.



Selezionare il formato **XLSX** per il report.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler bilanciare il carico sui tuoi volumi.

Crea un report per visualizzare gli aggregati che hanno il maggior numero di IOPS disponibili

Questo report mostra quali aggregati hanno il maggior numero di IOPS disponibili per tipo di aggregato su cui è possibile effettuare il provisioning di nuovi carichi di lavoro.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per aprire una vista Integrità: Tutti i volumi, scaricare la vista in Excel, creare un grafico della capacità disponibile, caricare il file Excel personalizzato e pianificare il report finale, procedere come segue.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > Aggregati**.
2. Selezionare **Prestazioni: Tutti gli aggregati** dal menu a discesa **Visualizza**.
3. Seleziona **Mostra/Nascondi** per mostrare il Available IOPS colonna e nascondi il Cluster FQDN, Inactive Data Reporting, E Threshold Policy colonne.
4. Trascina e rilascia il Available IOPS E Free Capacity colonne accanto al Type colonna.
5. Assegna un nome e salva la vista personalizzata Available IOPS Per Aggr.
6. Selezionare **Report > Scarica Excel**.



A seconda del browser utilizzato, potrebbe essere necessario fare clic su **OK** per salvare il file.

7. Se necessario, fare clic su **Abilita modifica**.

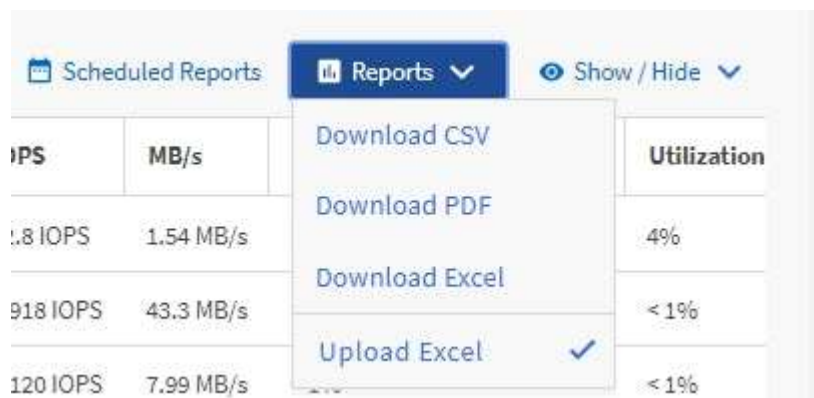
8. In Excel, apri il file scaricato.
9. Nel foglio dati, fare clic sul piccolo triangolo in alto a sinistra per selezionare l'intero foglio.
10. Sulla barra multifunzione **Dati**, seleziona **Ordina** da Sort & Filter area.
11. Imposta i seguenti livelli di ordinamento:
 - a. Specificare **Ordina per** come Available IOPS (IOPS), **Ordina su** come Cell Values, e l'**Ordine** come Largest to Smallest.
 - b. Fare clic su **Aggiungi livello**.
 - c. Specificare **Ordina per** come Type, **Ordina su** come Cell Values, e l'**Ordine** come Z to A.
 - d. Fare clic su **Aggiungi livello**.
 - e. Specificare **Ordina per** come Free Capacity (GB), **Ordina su** 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, seleziona **Report > Carica Excel**.



Assicurati di essere nella stessa vista in cui hai scaricato il file Excel.

14. Seleziona il file Excel che hai modificato, in questo caso performance-aggregates-<date>.xlsx.
15. Fare clic su **Apri**.
16. Fare clic su **Invia**.

Accanto alla voce di menu **Report > Carica Excel** appare un segno di spunta.



17. Fare clic su **Report pianificati**.
18. Fare clic su **Aggiungi pianificazione** per aggiungere una nuova riga alla pagina Pianificazioni report, in modo da poter definire le caratteristiche della pianificazione per il nuovo report.
19. Inserisci un nome per la pianificazione del report e completa gli altri campi del report, quindi fai clic sul segno di spunta (✓) alla fine della riga.



Selezionare il formato **XLSX** per il report.

Il rapporto viene inviato immediatamente a scopo di verifica. Successivamente, il report viene generato e inviato tramite e-mail ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potresti voler effettuare il provisioning di nuovi carichi di lavoro sugli aggregati che hanno il maggior numero di IOPS disponibili.

Gestire l'archiviazione utilizzando le API REST

Inizia con le API REST Active IQ Unified Manager

Active IQ Unified Manager fornisce un set di API per gestire le risorse di archiviazione sui sistemi di archiviazione supportati tramite un'interfaccia di servizio Web RESTful per qualsiasi integrazione di terze parti.

In questi argomenti troverai informazioni sulle API di Unified Manager, esempi di flussi di lavoro per risolvere problemi specifici e alcuni codici di esempio. Utilizzando queste informazioni, è possibile creare client RESTful delle soluzioni software NetApp Manageability per la gestione dei sistemi NetApp. Le API si basano sullo stile architetturale Representational State Transfer (REST). Sono supportate tutte e quattro le operazioni REST: Crea, Leggi, Aggiorna ed Elimina (note anche come CRUD).

Vedere "[Active IQ Unified Manager](#)" per risorse aggiuntive e dettagli sui vantaggi dell'API REST Active IQ Unified Manager.

Pubblico per questo contenuto

Gli argomenti trattati sono destinati agli sviluppatori che creano applicazioni che interagiscono con il software Active IQ Unified Manager tramite API REST.

Gli amministratori e gli architetti di storage possono fare riferimento a queste informazioni per acquisire una conoscenza di base su come utilizzare le API REST di Unified Manager per creare applicazioni client per gestire e monitorare i sistemi di storage NetApp.

È necessario utilizzare queste informazioni se si desidera utilizzare il provider di archiviazione, il cluster ONTAP e le API di amministrazione della gestione per gestire l'archiviazione.



È necessario disporre di uno dei seguenti ruoli: Operatore, Amministratore di archiviazione 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 e fornire oggetti di archiviazione nel proprio ambiente. È anche possibile accedere all'interfaccia utente Web di Unified Manager per eseguire alcune di queste funzioni.

Crea un URL per accedere direttamente alle API REST

È possibile accedere alle API REST direttamente tramite un linguaggio di programmazione, come Python, C#, C++, JavaScript e così via. Inserisci il nome host o l'indirizzo IP e l'URL per accedere alle API REST nel formato

`https://<nomehost>/api`



La porta predefinita è 443. È possibile configurare la porta in base alle esigenze del proprio ambiente.

Accedi alla pagina della documentazione API online

È possibile accedere alla pagina di riferimento *Documentazione API* fornita insieme al prodotto per visualizzare la documentazione API, nonché per emettere manualmente una chiamata API (sull'interfaccia, ad esempio, Swagger). È possibile accedere a questa documentazione cliccando sulla **Barra dei menu > Pulsante Aiuto > Documentazione API**

In alternativa, immettere il nome host o l'indirizzo IP e l'URL per accedere alla pagina REST API nel formato

`https://<nomehost>/docs/api/`

Categorie

Le chiamate API sono organizzate funzionalmente 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 ti aiutano a svolgere funzioni amministrative, di monitoraggio e di provisioning. Le API sono raggruppate nelle seguenti categorie.

- **centro dati**

Questa categoria contiene le API che ti aiutano nella gestione e nell'analisi dello storage del data center utilizzando strumenti come Work Flow Automation e Ansible. Le API REST in questa categoria forniscono informazioni su cluster, nodi, aggregati, volumi, LUN, condivisioni file, namespace e altri elementi nel data center.

- **server di gestione**

Le API nella categoria **management-server** contengono `jobs`, `system`, e `events` API. I job sono operazioni pianificate per l'esecuzione asincrona relative alla gestione di oggetti di archiviazione o carichi di lavoro su Unified Manager. IL `events` L'API restituisce eventi nel tuo data center e `system` L'API restituisce i dettagli dell'istanza di Unified Manager.

- **fornitore di storage**

Questa categoria contiene tutte le API di provisioning necessarie per la gestione e il provisioning di condivisioni file, LUN, livelli di servizio delle prestazioni e policy di efficienza dell'archiviazione. Le API consentono inoltre di configurare endpoint di accesso, Active Directory, nonché di assegnare livelli di servizio delle prestazioni e criteri di efficienza dell'archiviazione sui carichi di lavoro di archiviazione.

- **amministrazione**

Questa categoria contiene le API utilizzate per eseguire attività amministrative, come la gestione delle impostazioni di backup, la visualizzazione dei certificati di trust store per le origini dati di Unified Manager e la gestione dei cluster ONTAP come origini dati per Unified Manager.

- **portale**

Unified Manager consente di richiamare le API REST ONTAP tramite le API nella categoria gateway e di gestire gli oggetti di archiviazione nel data center.

- **sicurezza**

Questa categoria contiene le API per la gestione degli utenti di Unified Manager.

Servizi REST offerti in Active IQ Unified Manager

Prima di iniziare a utilizzare le API di Active IQ Unified Manager, è necessario conoscere i servizi e le operazioni REST offerti.

Le API di provisioning e amministrative utilizzate per configurare il server API supportano le operazioni di lettura (GET) o scrittura (POST, PATCH, DELETE). Di seguito sono riportati alcuni esempi delle operazioni GET, PATCH, POST e DELETE supportate dalle API:

- Esempio per GET: `GET /datacenter/cluster/clusters` recupera i dettagli del cluster nel tuo data center. Il numero massimo di record restituiti da GET l'operazione è 1000.



Le API consentono di filtrare, ordinare e classificare i record in base agli attributi supportati.

- Esempio per POST: `POST /datacenter/svm/svms` crea una macchina virtuale di archiviazione (SVM) personalizzata.
- Esempio per PATCH: `PATCH /datacenter/svm/svms/{key}` modifica le proprietà di una SVM, utilizzando la sua chiave univoca.
- Esempio per DELETE: `DELETE /storage-provider/access-endpoints/{key}` elimina un endpoint di accesso da una LUN, SVM o condivisione file utilizzando la sua chiave univoca.

Le operazioni REST che possono essere eseguite tramite le API dipendono dal ruolo dell'utente Operatore, Amministratore di archiviazione o Amministratore applicazione.

Ruolo utente	Metodo REST supportato
Operatore	Accesso ai dati in sola lettura. Gli utenti con questo ruolo possono eseguire tutte le richieste GET.
Amministratore di archiviazione	Accesso in lettura a tutti i dati. Gli utenti con questo ruolo possono eseguire tutte le richieste GET. Inoltre, dispongono di accesso in scrittura (per eseguire richieste PATCH, POST e DELETE) per svolgere attività specifiche, come la gestione di oggetti di servizi di archiviazione e opzioni di gestione dell'archiviazione.
Amministratore dell'applicazione	Accesso in lettura e scrittura a tutti i dati. Gli utenti con questo ruolo possono eseguire richieste GET, PATCH, POST e DELETE per tutte le funzioni.

Per maggiori informazioni su tutte le operazioni REST, consultare la *documentazione API online*.

Versione API in Active IQ Unified Manager

Gli URI dell'API REST in Active IQ Unified Manager specificano un numero di versione. Per esempio, `/v2/datacenter/svm/svms`. Il numero di versione `v2` in `/v2/datacenter/svm/svms` indica la versione API utilizzata in una versione 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 versioni future. Ad esempio, puoi trovare le stesse API anche 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 puoi selezionare la versione dell'API da utilizzare. Per impostazione predefinita viene selezionata la versione più alta. Si consiglia di utilizzare la versione più elevata di una determinata API (rispetto all'intero incrementale) disponibile nella propria istanza di Unified Manager.

Per tutte le richieste, è necessario richiedere esplicitamente la versione 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, dovresti includere il parametro versione. Dopo alcune release, le versioni precedenti delle API vengono deprecate. In questa versione, il `v1` la versione delle API è obsoleta.

Risorse di archiviazione in ONTAP

Le risorse di archiviazione in ONTAP possono essere ampiamente classificate in *risorse di archiviazione fisiche* e *risorse di archiviazione logiche*. Per gestire in modo efficace i sistemi ONTAP utilizzando le API fornite in Active IQ Unified Manager, è necessario comprendere il modello delle risorse di archiviazione e la relazione tra le varie risorse di archiviazione.

- **Risorse di archiviazione fisica**

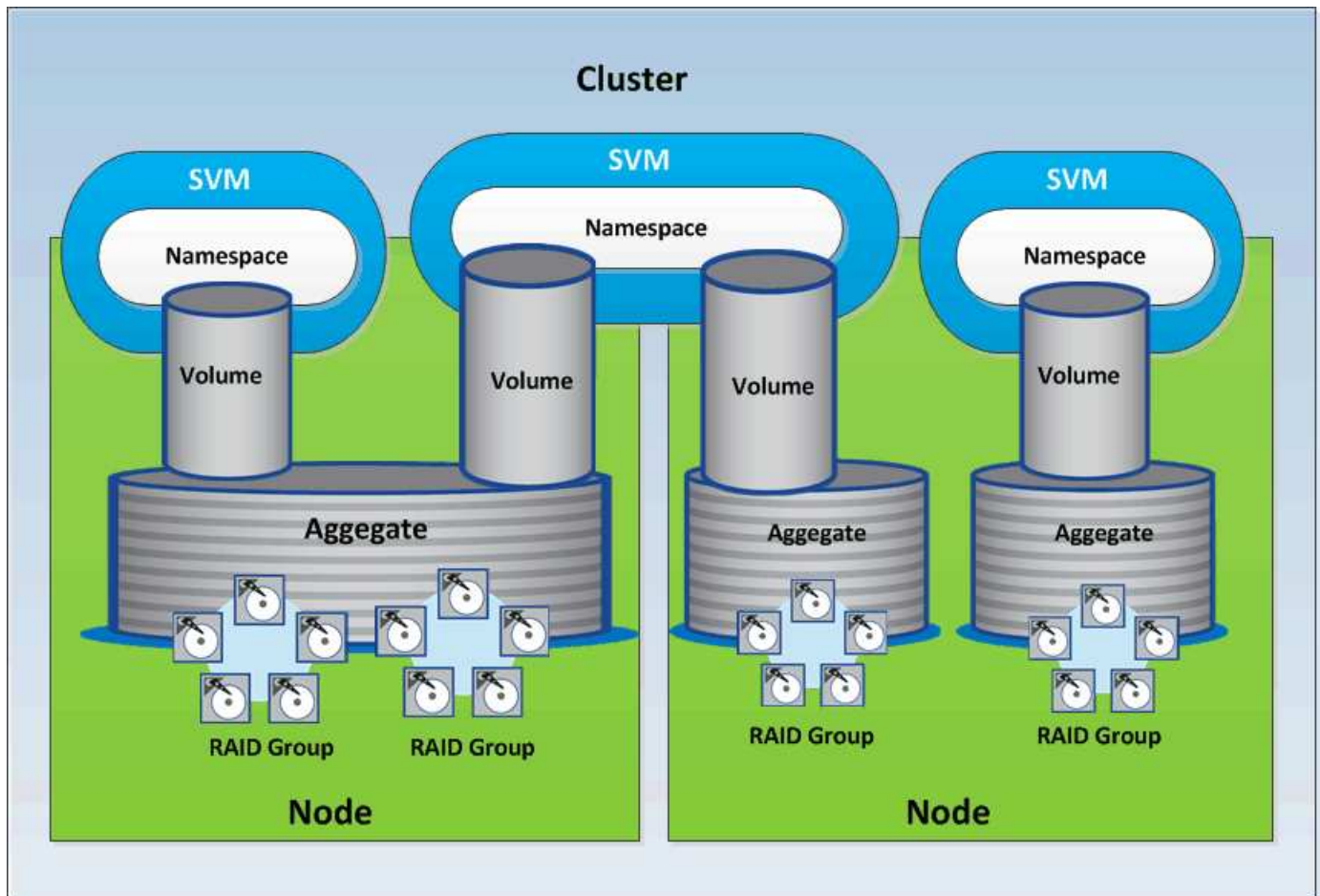
Si riferisce agli oggetti di archiviazione fisica forniti da ONTAP. Le risorse di archiviazione fisica includono dischi, cluster, controller di archiviazione, nodi e aggregati.

- **Risorse di archiviazione logica**

Si riferisce alle risorse di archiviazione fornite da ONTAP che non sono legate a una risorsa fisica. Queste risorse sono associate a una macchina virtuale di archiviazione (SVM, precedentemente nota come Vserver) ed esistono indipendentemente da qualsiasi risorsa di archiviazione fisica specifica, come un disco, un array LUN o un aggregato.

Le risorse di archiviazione logica includono volumi di tutti i tipi e qtree, nonché le funzionalità e le configurazioni che è possibile utilizzare con queste risorse, come copie snapshot, deduplicazione, compressione e quote.

L'illustrazione seguente mostra le risorse di archiviazione in un cluster a 2 nodi:



Accesso e autenticazione API REST in Active IQ Unified Manager

L'API REST Active IQ Unified Manager è accessibile tramite qualsiasi client REST o piattaforma di programmazione in grado di inviare richieste HTTP con un meccanismo di autenticazione HTTP di base.

Esempio di richiesta e risposta:

- **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 plugin del browser REST API. È possibile accedere alla REST API anche 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 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 è stato configurato il server API per l'autenticazione tramite LDAP). È possibile gestire l'accesso degli utenti effettuando l'accesso all'interfaccia utente della console di amministrazione di Unified Manager.

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 di Active IQ Unified Manager .

Nella tabella seguente sono elencati i codici di errore relativi all'autenticazione:

Codice di stato HTTP	Titolo del codice di stato	Descrizione
200	OK	Restituito in caso di esecuzione corretta delle chiamate API sincrone.
201	Creato	Creazione di nuove risorse tramite chiamate sincrone, come 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 nella convalida dell'input. L'utente deve correggere gli input, ad esempio le chiavi valide nel corpo di una richiesta.
401	Richiesta non autorizzata	Non sei autorizzato a visualizzare la risorsa/Non autorizzato.
403	Richiesta proibita	L'accesso alla risorsa che stavi cercando 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	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 esegui un <code>GET</code> O <code>GET ALL</code> operazione e si riceve questo errore, si consiglia di ripetere l'operazione per almeno cinque tentativi. Se si tratta di un errore permanente, il codice di stato restituito continua a essere 500. Se l'operazione riesce, il codice di stato restituito è 200.

Consigli 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. Dovresti utilizzare la versione più recente dell'API disponibile per la tua istanza di Unified Manager. Per ulteriori informazioni sulle versioni dell'API di Unified Manager, vedere la sezione "Versione dell'API REST in Active IQ Unified Manager".
- Durante l'aggiornamento dei valori dell'array tramite un'API 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 operatori di filtro, come pipe (|) e caratteri jolly (*), per tutti i parametri di query, ad eccezione dei valori double, ad esempio IOPS e prestazioni nelle API delle metriche.
- Evitare di interrogare gli oggetti utilizzando una combinazione degli operatori di filtro jolly (*) e barra verticale (|). Potrebbe recuperare un numero errato di oggetti.
- Quando si utilizzano valori per il filtro, assicurarsi che il valore non contenga alcun ? carattere. Questo serve a mitigare i rischi di iniezione SQL.
- Nota che il `GET` (tutte) le richieste per qualsiasi API restituiscono un massimo di 1000 record. Anche se si esegue la query impostando `max_records` parametro su un valore superiore a 1000, vengono restituiti solo 1000 record.
- Per eseguire 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 degli errori e di risolvere i problemi

che potrebbero verificarsi durante l'esecuzione delle API.

Recupera i registri dalla seguente posizione per risolvere i problemi relativi alle chiamate API.

Posizione del registro	Utilizzo
<code>/var/log/ocie/access_log.log</code>	Contiene tutti i dettagli della chiamata API, come 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 registro per controllare le API utilizzate di frequente o per risolvere i problemi di qualsiasi flusso di lavoro GUI. È possibile utilizzarlo anche per scalare l'analisi in base al tempo di esecuzione.
<code>/var/log/ocum/ocumserver.log</code>	Contiene tutti i log di esecuzione dell'API. È possibile utilizzare questo file di registro per risolvere i problemi e per eseguire il debug delle chiamate API.
<code>/var/log/ocie/server.log</code>	Contiene tutte le distribuzioni del server Wildfly e i registri relativi all'avvio/arresto del servizio. È possibile utilizzare questo file di registro per individuare la causa principale di eventuali problemi che si verificano durante l'avvio, l'arresto o la distribuzione del server Wildfly.
<code>/var/log/ocie/au.log</code>	Contiene i registri relativi all'unità di acquisizione. È possibile utilizzare questo file di registro quando si creano, modificano o eliminano oggetti in ONTAP , ma questi non vengono riflessi per le API REST Active IQ Unified Manager .

Processi asincroni degli oggetti di lavoro

Active IQ Unified Manager fornisce `jobs` API che recupera informazioni sui lavori eseguiti durante l'esecuzione di altre API. È necessario sapere come funziona l'elaborazione asincrona utilizzando l'oggetto Job.

Alcune chiamate API, in particolare quelle utilizzate per aggiungere o modificare risorse, possono richiedere più tempo per essere completate rispetto ad altre chiamate. Unified Manager elabora queste richieste di lunga durata 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 è ancora stata completata. La richiesta viene elaborata come un'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 suo identificatore univoco.

Interroga l'oggetto Job associato a una richiesta API

L'oggetto Job restituito nella risposta HTTP contiene diverse proprietà. È possibile interrogare la proprietà di stato 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 interroga un oggetto Job per rilevare uno stato terminale per l'attività, ovvero successo o fallimento:

- Richiesta di polling standard: lo stato corrente del Job viene restituito immediatamente.
- Richiesta di polling lungo: quando lo stato del lavoro passa a NORMAL, ERROR, O PARTIAL_FAILURES.

Fasi di una richiesta asincrona

Per completare una chiamata API asincrona, è possibile utilizzare la seguente procedura di alto livello:

1. Emettere la chiamata API asincrona.
2. Ricevere una risposta HTTP 202 che indica l'accettazione corretta della richiesta.
3. Estrarre l'identificatore per l'oggetto Job dal corpo della risposta.
4. All'interno di un ciclo, attendi che l'oggetto Job raggiunga lo stato terminale NORMAL, ERROR, O PARTIAL_FAILURES.
5. Verificare lo stato terminale del Job e recuperare il risultato del Job.

Ciao server API

Il server *Hello API* 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 dettagli di base sul server API nel formato JSON (il server supporta solo `application/json` formato).

L'URI utilizzato è: <https://<hostname>/api/datacenter/svm/svms>. Questo codice di esempio accetta i seguenti parametri di input:

- L'indirizzo IP del server API o FQDN
- Facoltativo: numero di porta (predefinito: 443)
- Nome utente
- Password
- Formato di risposta(`application/json`)

Per richiamare le API REST, è possibile utilizzare anche altri script, come Jersey e RESTEasy, per scrivere un

client Java REST per Active IQ Unified Manager. È opportuno tenere presente le seguenti considerazioni sul codice di esempio:

- Utilizza una connessione HTTPS ad Active IQ Unified Manager per richiamare l'URI REST specificato
- Ignora il certificato fornito da Active IQ Unified Manager
- Salta la verifica del nome host durante l'handshake
- Usi `javax.net.ssl.HttpsURLConnection` per una connessione URI
- Utilizza una libreria di terze parti(`org.apache.commons.codec.binary.Base64`) per costruire la 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 HttpURLConnection
getAllTrustingHttpsURLConnection() {
    HttpURLConnection 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());
URLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));
URL url = new URL(server_url);
conn =
(HttpURLConnection) 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

In questa sezione sono elencate le API REST per Active IQ Unified Manager , in base alle rispettive categorie.

È possibile visualizzare la pagina della documentazione online dalla propria istanza di Unified Manager, che include i dettagli di ogni chiamata API REST. Il presente 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 esaminarne i dettagli completi, inclusi i parametri di input, i formati di output, i codici di stato HTTP e il tipo di elaborazione della richiesta.

Per ogni chiamata API all'interno di un flusso di lavoro sono incluse le seguenti informazioni, che aiutano a individuare la chiamata nella pagina della documentazione:

- Categoria

Le chiamate API sono organizzate nella pagina della documentazione in aree o categorie correlate dal punto di vista funzionale. Per individuare una chiamata API specifica, scorrere 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.

- Sentiero

Il percorso determina la risorsa specifica che 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.

Gestire gli oggetti di archiviazione in un data center utilizzando le API

Le API REST sotto `datacenter` La categoria consente di gestire gli oggetti di archiviazione nel data center, come cluster, nodi, aggregati, VM di archiviazione, volumi, LUN, condivisioni di file e namespace. Queste API sono disponibili per interrogare la configurazione degli oggetti, mentre alcune di esse consentono di eseguire operazioni di aggiunta, eliminazione o modifica di tali oggetti.

La maggior parte di queste API sono chiamate GET che forniscono aggregazione tra cluster con supporto per filtraggio, ordinamento e impaginazione. Eseguendo queste API, vengono restituiti dati dal database. Pertanto, gli oggetti appena creati devono essere scoperti dal successivo ciclo di acquisizione per poter apparire nella risposta.

Se si desidera interrogare i dettagli di un oggetto specifico, è necessario immettere l'ID univoco di tale oggetto per visualizzarne i dettagli. Ad esempio, per le informazioni sulle metriche e le analisi degli oggetti di archiviazione, vedere ["Visualizzazione delle metriche delle prestazioni"](#).

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```



I comandi CURL, gli esempi, le richieste e le risposte alle API sono disponibili nell'interfaccia API Swagger. È possibile filtrare e ordinare i risultati in base a parametri specifici, come indicato su Swagger. Queste API consentono di filtrare i risultati per oggetti di archiviazione specifici, come cluster, volumi o VM di archiviazione.

API per oggetti di archiviazione nel tuo data center

Verbo HTTP	Sentiero	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, come l'indirizzo IPv4 o IPv6 del cluster, informazioni sul nodo, come lo stato del nodo, la capacità delle prestazioni e la coppia di alta disponibilità (HA) e indica se il cluster è un array All SAN.
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	Restituisce i dettagli delle licenze installate sui cluster nel tuo data center. Puoi 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 immettere 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 prestazioni e sulla coppia di alta disponibilità (HA) 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 su cluster, SVM e volume, vengono restituite anche informazioni sull'elenco di controllo degli accessi (ACL).

Verbo HTTP	Sentiero	Descrizione
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 interrogare i criteri di esportazione per un cluster o una VM di archiviazione e riutilizzare la chiave del criterio di esportazione per il provisioning delle condivisioni file NFS. Per ulteriori informazioni sull'assegnazione e il riutilizzo dei criteri di esportazione sui carichi di lavoro, vedere "Provisioning di condivisioni file CIFS e NFS".
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	È possibile utilizzare questo metodo per visualizzare la raccolta di aggregati nel data center o un aggregato specifico per il provisioning dei carichi di lavoro su di essi o per il monitoraggio. Vengono restituite informazioni quali dettagli su cluster e nodi, capacità prestazionale utilizzata, spazio disponibile e utilizzato ed efficienza di archiviazione.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	È possibile utilizzare questo metodo per visualizzare la raccolta di LUN nell'intero data center. È possibile visualizzare informazioni sulla LUN, come dettagli sul cluster e sulla SVM, criteri QoS e igroup.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli di tutti i criteri QoS applicabili agli oggetti di archiviazione nel data center. Vengono restituite informazioni quali i dettagli del cluster e dell'SVM, i dettagli della policy fissa o adattiva e il numero di oggetti applicabili a tale policy.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees /{key}	È possibile utilizzare questo metodo per visualizzare i dettagli qtree nel data center per tutti i volumi FlexVol o FlexGroup . Vengono restituite informazioni quali i dettagli del cluster e dell'SVM, il FlexVol volume e la policy di esportazione.
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 dettagli SVM e cluster, QoS e policy di esportazione, se il volume è di tipo lettura-scrittura, protezione dati o condivisione del carico. 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	Sentiero	Descrizione
GET POST DELETE PATCH	/datacenter/protocols/san/ igroups /datacenter/protocols/san/ igroups/{key}	È possibile assegnare gruppi di iniziatori (igroup) autorizzati ad accedere a specifiche destinazioni LUN. Se esiste già un igroup, è possibile assegnarlo. È anche possibile creare igroup e assegnarli ai LUN. È possibile utilizzare questi metodi per interrogare, creare, eliminare e modificare rispettivamente gli igroup. Punti da notare: • `POST`: Durante la creazione di un igroup, è possibile designare la VM di archiviazione a cui si desidera assegnare l'accesso. • `DELETE`: Per eliminare un particolare igroup è necessario fornire la chiave igroup come parametro di input. Se hai già assegnato un igroup a una LUN, non puoi eliminare quell'igroup. • `PATCH`: Per modificare un particolare igroup è necessario fornire la chiave igroup come parametro di input. È necessario inserire anche la proprietà che si desidera aggiornare, insieme al suo valore.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/svm/svms	È possibile utilizzare questi metodi per visualizzare, creare, eliminare e modificare le macchine virtuali di archiviazione (VM di archiviazione). • POST: È necessario immettere l'oggetto VM di archiviazione che si desidera creare come parametro di input. È possibile creare una VM di archiviazione personalizzata e quindi assegnarle le proprietà richieste. • DELETE: Per eliminare una determinata VM di archiviazione, è necessario fornire la chiave della VM di archiviazione. • PATCH: Per modificare una determinata VM di archiviazione è necessario fornire la chiave della VM di archiviazione. È inoltre necessario immettere le proprietà che si desidera aggiornare, insieme ai relativi valori.
POST	/datacenter/svm/svms/{key}	
DELETE		
PATCH		



Punti da notare:

Se hai abilitato il provisioning del carico di lavoro basato su SLO nel tuo ambiente, durante la creazione della VM di archiviazione, assicurati che supporti tutti i protocolli richiesti per il provisioning di LUN e condivisioni file su di esse, ad esempio CIFS o SMB, NFS, FCP e iSCSI. I flussi di lavoro di provisioning potrebbero non funzionare se la VM di archiviazione non supporta i servizi richiesti. Si consiglia di abilitare i servizi per i rispettivi tipi di carichi di lavoro anche sulla VM di archiviazione.

Se hai abilitato il provisioning dei carichi di lavoro basato su SLO nel tuo ambiente, non puoi eliminare la VM di archiviazione su cui sono stati eseguiti il provisioning dei carichi di lavoro di archiviazione. Quando si elimina una VM di archiviazione 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 a essere presente nella configurazione di Active Directory e deve essere eliminato manualmente dal server Active Directory.

API per gli elementi di rete nel tuo data center

Le seguenti API nella categoria datacenter recuperano informazioni sulle porte e sulle interfacce di rete nel tuo ambiente, in particolare sulle porte FC, sulle interfacce FC, sulle porte Ethernet e sulle interfacce IP.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Recupera informazioni su tutte le porte Ethernet presenti nel tuo ambiente data center. Utilizzando una chiave di porta come parametro di input, è possibile visualizzare le informazioni di quella porta specifica. Vengono recuperate informazioni quali dettagli del cluster, dominio di broadcast, dettagli della porta, come stato, velocità e tipo, e se la porta è abilitata.
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. Utilizzando una chiave di interfaccia come parametro di input, è possibile visualizzare le informazioni di quella specifica interfaccia. Vengono recuperate informazioni quali i dettagli del cluster, i dettagli del nodo home e i dettagli della porta home.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Recupera informazioni su tutte le porte FC utilizzate nei nodi nell'ambiente del data center. Utilizzando una chiave di porta come parametro di input, è possibile visualizzare le informazioni di quella porta specifica. Vengono recuperate informazioni quali i dettagli del cluster, la descrizione della porta, il protocollo supportato e lo stato della porta.

Verbo HTTP	Sentiero	Descrizione
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. Utilizzando una chiave di interfaccia come parametro di input, è possibile visualizzare le informazioni di quella specifica interfaccia. Vengono recuperate informazioni quali i dettagli del cluster, i dettagli dello spazio IP, i dettagli del nodo home e se il failover è abilitato.

Accedi alle API ONTAP tramite accesso proxy

Le API gateway offrono il vantaggio di utilizzare le credenziali di Active IQ Unified Manager per eseguire le API REST ONTAP e gestire gli oggetti di archiviazione. Queste API sono disponibili quando la funzionalità API Gateway è abilitata 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 usufruire delle altre funzionalità tramite le API ONTAP. Le API gateway consentono a Unified Manager di fungere da interfaccia pass-through per l'instradamento di tutte le richieste API da eseguire sui cluster ONTAP che gestisce, senza dover accedere singolarmente a ciascun cluster del data center. Funziona come un unico punto di gestione per l'esecuzione delle API nei cluster ONTAP gestiti dall'istanza di Unified Manager. La funzionalità API Gateway consente a Unified Manager di essere un unico piano di controllo da cui è possibile gestire più cluster ONTAP, senza doverli accedere singolarmente. Le API gateway consentono di rimanere connessi a Unified Manager e di gestire i cluster ONTAP eseguendo le operazioni dell'API REST ONTAP.



Tutti gli utenti possono eseguire una query utilizzando l'operazione GET. Gli amministratori dell'applicazione possono eseguire tutte le operazioni ONTAP REST.

Il gateway funge da proxy per incanalare le richieste API mantenendo l'intestazione e il corpo delle richieste 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 dover passare le credenziali individuali del cluster. Continua a gestire l'autenticazione e la gestione del cluster, ma reindirizza le richieste API per eseguirle 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 ONTAP REST. È possibile verificare i dettagli del cluster e scegliere di eseguire altri metodi in base all'UUID del cluster o all'identificatore univoco universale (UUID).  Le API del gateway recuperano solo i cluster supportati da ONTAP 9.5 o versioni successive e aggiunti a Unified Manager tramite HTTPS.
GET POST DELETE PATCH OPTIONS(non disponibile su Swagger) HEAD(non disponibile su Swagger)	/gateways/{uuid}/{path}  Il valore per {uuid} deve essere sostituito con l'UUID del cluster su cui deve essere eseguita l'operazione REST. Inoltre, assicurarsi che l'UUID appartenga al cluster supportato da ONTAP 9.5 o versione successiva e aggiunto a Unified Manager tramite HTTPS. {path} deve essere sostituito dall'URL REST ONTAP . Devi rimuovere /api/ dall'URL.	Si tratta di un'API proxy a punto singolo, che supporta le operazioni POST, DELETE, PATCH e GET per tutte le API REST ONTAP . Non si applicano restrizioni su nessuna API, purché sia supportata da ONTAP. La funzionalità di tunneling o proxy non può essere disabilitata. IL OPTIONS Il metodo restituisce tutte le operazioni supportate da un'API REST ONTAP . Ad esempio, se un'API ONTAP supporta solo GET operazione, esecuzione del OPTIONS metodo utilizzando questa API gateway restituisce GET come risposta. Questo metodo non è supportato su Swagger, ma può essere eseguito su altri strumenti API. IL OPTIONS metodo determina se una risorsa è disponibile. Questa operazione può essere utilizzata per visualizzare i metadati relativi a una risorsa nelle intestazioni di risposta HTTP. Questo metodo non è supportato su Swagger, ma può essere eseguito su altri strumenti API.

Comprendere il tunneling dell'API Gateway

Le API 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 ONTAP. L'API gateway trasforma l'URL e i collegamenti Hypermedia as the Engine of Application State (HATEOAS) nell'intestazione e nel corpo della risposta con l'URL di base del gateway API. L'API gateway funge da URL di base proxy a cui aggiungere l'URL REST ONTAP ed eseguire l'endpoint REST ONTAP richiesto.



Affinché un'API ONTAP venga eseguita correttamente tramite 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 dell'API ONTAP come valore per il parametro path.



Quando aggiungi il percorso, assicurati di aver rimosso “/” symbol at the beginning of the URL. For the API `/storage/volumes`, aggiungere `storage/volumes`.

L'URL aggiunto è: `/gateways/{uuid}/storage/volumes`

Durante l'esecuzione del 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 aggiunto e quello per l'API gateway viene mantenuto.

Esempio di comando cURL

```
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 archiviazione in quel cluster. Il formato della risposta è lo stesso che si riceve quando si esegue la stessa API da ONTAP. I codici di stato restituiti sono i codici di stato REST ONTAP.

Imposta l'ambito dell'API

Tutte le API hanno un contesto impostato all'interno dell'ambito del cluster. Anche le API che operano sulla base di VM di storage hanno come ambito il cluster, ovvero le operazioni API vengono eseguite su una particolare VM di storage all'interno di un cluster gestito. Quando esegui il `/gateways/{uuid}/{path}` API, assicurati di immettere l'UUID del cluster (UUID dell'origine dati Unified Manager) per il cluster su cui esegui l'operazione. Per impostare il contesto su una specifica VM di archiviazione all'interno di quel cluster, immettere la chiave della VM di archiviazione come parametro `X-Dot-SVM-UUID` oppure il nome della VM di archiviazione come parametro `X-Dot-SVM-Name`. Il parametro viene aggiunto come filtro nell'intestazione della stringa e l'operazione viene eseguita nell'ambito di quella VM di archiviazione all'interno di quel cluster.

Esempio di comando cURL


```
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 ONTAP , vedere <https://docs.netapp.com/us-en/ontap-automation/index.html> ["Automazione API REST ONTAP"]

Eseguire attività amministrative utilizzando le API

È possibile utilizzare le API sotto `administration` categoria per modificare le impostazioni di backup, verificare le informazioni sui 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. Per configurare queste impostazioni è possibile utilizzare anche l'interfaccia utente Web di Unified Manager.

Verbo HTTP	Sentiero	Descrizione
GET	/admin/backup-settings	Puoi usare il GET metodo per visualizzare le impostazioni della pianificazione del backup configurata per impostazione predefinita in Unified Manager. Puoi verificare quanto segue: • Se la pianificazione è abilitata o disabilitata • Frequenza del backup pianificato (giornaliera o settimanale) • Ora del backup • Numero massimo di file di backup che devono essere conservati nell'applicazione L'ora del backup è espressa nel fuso orario del server. Le impostazioni di backup del database sono disponibili per impostazione predefinita su Unified Manager e non è possibile creare una pianificazione di backup. Tuttavia, è possibile utilizzare il PATCH metodo per modificare le impostazioni predefinite.
PATCH	/admin/backup-settings	

Verbo HTTP	Sentiero	Descrizione
GET	/admin/backup-file-info	Ogni volta che viene modificata la pianificazione del backup per Unified Manager, viene generato un file di dump del backup. È possibile utilizzare questo metodo per verificare se il file di backup è stato 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 attendibile. La convalida del certificato è obbligatoria prima di aggiungere un cluster ONTAP come origine dati Unified Manager.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Puoi usare il GET metodo per recuperare i dettagli delle origini dati (cluster ONTAP) gestite da Unified Manager. È anche 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 .

Gestisci gli utenti tramite 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 del database. È anche possibile aggiungere utenti o gruppi remoti che appartengono a un server di autenticazione. In base ai privilegi dei ruoli assegnati agli utenti, questi possono gestire gli oggetti di archiviazione o visualizzare i dati in Unified Manager.



Per eseguire queste operazioni è necessario disporre del ruolo di Amministratore dell'applicazione. Per configurare queste impostazioni è possibile utilizzare anche l'interfaccia utente Web di Unified Manager.

Le API sotto il `security` categoria utilizza il parametro `utenti`, ovvero il nome utente, e non il parametro chiave come identificatore univoco per l'entità utente.

Verbo HTTP	Sentiero	Descrizione
GET POST	 /security/users	È possibile utilizzare questi metodi per ottenere i dettagli degli utenti o aggiungere nuovi utenti a Unified Manager. È possibile aggiungere ruoli specifici agli utenti in base alla loro tipologia. Quando si aggiungono utenti, è necessario fornire le password per l'utente locale, l'utente addetto alla manutenzione e l'utente del database.
GET PATCH DELETE	 /security/users/{name}	Il metodo GET consente di recuperare tutti i dettagli di un utente, come nome, indirizzo email, ruolo, tipo di autorizzazione. Il metodo PATCH consente di aggiornare i dettagli. Il metodo DELETE consente di rimuovere l'utente.

Visualizza le metriche delle prestazioni utilizzando le API

Active IQ Unified Manager ti fornisce un set di API sotto `/datacenter` categoria che consente di visualizzare i dati sulle prestazioni dei cluster e degli oggetti di archiviazione in un data center. Queste API recuperano i dati sulle prestazioni dei diversi oggetti di archiviazione, quali cluster, nodi, LUN, volumi, aggregati, VM di archiviazione, interfacce FC, porte FC, porte Ethernet e interfacce IP.

IL `/metrics` E `/analytics` Le API forniscono diverse visualizzazioni delle metriche delle prestazioni, tramite le quali è possibile accedere a diversi livelli di dettaglio per i seguenti oggetti di archiviazione nel data center:

- cluster
- nodi
- VM di archiviazione
- aggregati
- volumi
- LUN

- Interfacce FC
- porte FC
- porte Ethernet
- Interfacce IP

La tabella seguente traccia un confronto tra `/metrics` E `/analytics` API relative ai dettagli dei dati sulle prestazioni recuperati.

Metrica	Analisi
Dettagli sulle prestazioni per un singolo oggetto. Ad esempio, il <code>/datacenter/cluster/clusters/{key}/metrics</code> L'API richiede che la chiave del cluster venga inserita come parametro del percorso per recuperare le metriche per quel cluster specifico.	Dettagli sulle prestazioni per più oggetti dello stesso tipo in un data center. Ad esempio, il <code>/datacenter/cluster/clusters/analytics</code> L'API recupera le metriche collettive di tutti i cluster in un data center.
Esempio di metriche delle prestazioni per un oggetto di archiviazione basato sul parametro dell'intervallo di tempo per il recupero.	Valore aggregato di alto livello delle prestazioni per un determinato tipo di oggetto di archiviazione per un determinato periodo (oltre 72 ore).
Vengono recuperati i dettagli di base dell'oggetto, come i dettagli di un nodo o di un cluster.	Non sono stati recuperati dettagli specifici.
I contatori accumulati, come i valori minimo, massimo, 95° percentile e medio delle prestazioni in un periodo di tempo, vengono recuperati per un singolo oggetto, come contatori di lettura, scrittura, totale e altri.	Per tutti gli oggetti dello stesso tipo viene visualizzato un singolo valore aggregato.

Metrica	Analisi
L'intervallo di tempo e i dati campione si basano sulla seguente pianificazione: Intervallo di tempo per i dati. Gli esempi possono essere 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m. Si ottengono campioni di 1 ora se l'intervallo è superiore a 3 giorni (72 ore), altrimenti si ottengono campioni di 5 minuti. Il periodo per ciascun intervallo di tempo è il seguente: • 1h: metriche relative all'ora più recente, campionate in 5 minuti. • 12h: metriche delle ultime 12 ore campionate in 5 minuti. • 1d: Metriche relative al giorno più recente 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 degli ultimi 15 giorni campionate in 1 ora. • 1w: metriche della settimana più recente campionate in 1 ora. • 1m: metriche del mese più recente campionate in 1 ora. • 2m: metriche degli ultimi 2 mesi campionate in 1 ora. • 3m: metriche degli ultimi 3 mesi campionate in 1 ora. • 6m: metriche degli ultimi 6 mesi campionate in 1 ora. Valori disponibili: 1h, 12h, 1g, 2g, 3g, 15g, 1w, 1m, 2m, 3m, 6m Valore predefinito: 1h	Oltre le 72 ore. La durata su cui viene calcolato questo campione è rappresentata nel formato standard ISO-8601.

Esempio di output per le API delle metriche

Ad esempio, il `/datacenter/cluster/nodes/{key}/metrics` L'API recupera i seguenti dettagli (tra gli altri) per un nodo:



Il 95° percentile nel valore riepilogativo indica che il 95% dei campioni raccolti nel periodo ha un valore 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` L'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 tabella seguente descrive il `/metrics` E `/analytics` API in dettaglio.



Gli IOPS e le metriche delle prestazioni restituiti da queste API sono valori doppi, ad esempio 100.53 . Il filtraggio di questi valori float tramite i caratteri barra verticale (|) e carattere jolly (*) non è supportato.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/cluster/clusters/{key}/metrics	Recupera i dati sulle prestazioni (campione e riepilogo) per un cluster specificato dal parametro di input della chiave del cluster. Vengono restituite informazioni quali la chiave del cluster e l'UUID, l'intervallo di tempo, gli IOPS, la produttività e il numero di campioni.
GET	/datacenter/cluster/clusters/analytics	Recupera metriche di prestazioni di alto livello per tutti i cluster in un data center. Puoi filtrare i risultati in base ai criteri richiesti. Vengono restituiti valori quali IOPS aggregati, produttività e periodo di raccolta (in ore).
GET	/datacenter/cluster/nodes/{key}/metrics	Recupera i dati sulle prestazioni (campione e riepilogo) per un nodo specificato dal parametro di input della chiave del nodo. Vengono restituite informazioni quali l'UUID del nodo, l'intervallo di tempo, il riepilogo degli IOPS, la produttività, la latenza e le prestazioni, il numero di campioni raccolti e la percentuale utilizzata.
GET	/datacenter/cluster/nodes/analytics	Recupera parametri di prestazioni di alto livello per tutti i nodi di un data center. Puoi filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni, come chiavi di nodi e cluster, e valori, come IOPS aggregati, produttività e periodo di raccolta (in ore).
GET	/datacenter/storage/aggregates/{key}/metrics	Recupera i dati sulle prestazioni (campione e riepilogo) per un aggregato specificato dal parametro di input della chiave di aggregazione. Vengono restituite informazioni quali l'intervallo di tempo, il riepilogo degli IOPS, la latenza, la produttività e la capacità prestazionale, il numero di campioni raccolti per ciascun contatore e la percentuale utilizzata.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/storage/aggregates/analytics	Recupera metriche di prestazioni di alto livello per tutti gli aggregati in un data center. Puoi filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni quali chiavi aggregate e cluster e valori quali 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 file (volume) specificata dal parametro di input della LUN o della chiave del volume. Vengono restituite informazioni quali il riepilogo del minimo, del massimo e della media degli IOPS di lettura, scrittura e totali, della latenza e della produttività, nonché il numero di campioni raccolti per ciascun contatore.
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	Recupera metriche di prestazioni di alto livello per tutti i LUN o volumi in un data center. Puoi 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 prestazioni (campione e riepilogo) per una VM di archiviazione specificata dal parametro di input della chiave della VM di archiviazione. Riepilogo degli IOPS in base a ciascun protocollo supportato, come ad esempio <code>nvmf</code> , <code>fcp</code> , <code>iscsi</code> , <code>Nfs</code> , vengono restituiti la produttività, la latenza e il numero di campioni raccolti.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/svm/svms/analytics	Recupera metriche di prestazioni di alto livello per tutte le VM di archiviazione in un data center. Puoi filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni quali UUID della VM di archiviazione, IOPS aggregati, latenza, throughput e periodo di raccolta (in ore).
GET	/datacenter/network/ethernet/ports/{key}/metrics	Recupera le metriche delle prestazioni per una specifica porta Ethernet 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, come i valori minimi, massimi e medi delle prestazioni nel periodo di tempo.
GET	/datacenter/network/ethernet/ports/analytics	Recupera le metriche delle prestazioni di alto livello per tutte le porte Ethernet nell'ambiente del tuo data center. Vengono restituite informazioni quali la chiave del cluster e del nodo e l'UUID, la produttività, il periodo di raccolta e la percentuale di utilizzo delle porte. È possibile filtrare il risultato in base ai parametri disponibili, come 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 prestazioni per una specifica interfaccia di rete FC specificata dal parametro di input della chiave dell'interfaccia. Quando viene fornito un intervallo (intervallo di tempo) dall'intervallo supportato, l'API restituisce i contatori accumulati, come i valori minimi, massimi e medi delle prestazioni nel periodo di tempo.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/network/fc/interfaces/analytics	Recupera le metriche delle prestazioni di alto livello per tutte le porte Ethernet nell'ambiente del tuo data center. Vengono restituite informazioni quali la chiave dell'interfaccia FC e del cluster, l'UUID, la velocità effettiva, gli IOPS, la latenza e la VM di archiviazione. È possibile filtrare il risultato in base ai parametri disponibili, come il nome e l'UUID dell'interfaccia del cluster e FC, la VM di archiviazione, la velocità effettiva e così via.
GET	/datacenter/network/fc/ports/{key}/metrics	Recupera le metriche delle prestazioni per una specifica porta FC 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, come i valori minimi, massimi e medi delle prestazioni nel periodo di tempo.
GET	/datacenter/network/fc/ports/analytics	Recupera le metriche delle prestazioni di alto livello per tutte le porte FC nell'ambiente del data center. Vengono restituite informazioni quali la chiave del cluster e del nodo e l'UUID, la produttività, il periodo di raccolta e la percentuale di utilizzo delle porte. È possibile filtrare il risultato in base ai parametri disponibili, come la chiave della porta, la percentuale di utilizzo, il nome del cluster e del nodo, l'UUID e così via.

Verbo HTTP	Sentiero	Descrizione
GET	/datacenter/network/ip/interfaces/{key}/metrics	Recupera le metriche delle prestazioni per un'interfaccia IP di rete come specificato dal parametro di input della chiave dell'interfaccia. Quando viene fornito un intervallo (intervallo di tempo) dall'intervallo supportato, l'API restituisce informazioni quali il numero di campioni, i contatori accumulati, la produttività e il numero di pacchetti ricevuti e trasmessi.
GET	/datacenter/network/ip/interfaces/analytics	Recupera le metriche delle prestazioni di alto livello per tutte le interfacce IP di rete nell'ambiente del tuo data center. Vengono restituite informazioni quali la chiave dell'interfaccia IP e del cluster, l'UUID, la velocità effettiva, gli IOPS e la latenza. È possibile filtrare il risultato in base ai parametri disponibili, come il nome del cluster e dell'interfaccia IP e UUID, IOPS, latenza, throughput e così via.

Visualizza i lavori e i dettagli del sistema

Puoi usare il `jobs` API sotto il `management-server` categoria per visualizzare i dettagli di esecuzione delle operazioni asincrone. IL `system` API sotto il `management-server` La categoria consente di visualizzare i dettagli dell'istanza nel tuo ambiente Active IQ Unified Manager .

Visualizza lavori

In Active IQ Unified Manager, le operazioni, come l'aggiunta e la modifica delle risorse, vengono eseguite tramite 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 ha una chiave univoca per l'identificazione. Ogni oggetto Job restituisce l'URI dell'oggetto Job per consentirti di accedere e monitorare l'avanzamento del lavoro. È possibile utilizzare questa API per recuperare i dettagli di ogni esecuzione.

Utilizzando questa API, puoi interrogare tutti gli oggetti Job per il tuo data center, inclusi i dati storici. Per impostazione predefinita, l'interrogazione di tutti i lavori restituisce i dettagli degli ultimi 20 lavori attivati tramite l'interfaccia utente Web e l'interfaccia API. Utilizza i filtri integrati per visualizzare lavori specifici. È anche possibile utilizzare il tasto Job per interrogare i dettagli di un job specifico ed eseguire il set successivo di operazioni sulle risorse.

Categoria	Verbo HTTP	Sentiero	Descrizione
server di gestione	OTTENERE	/management-server/jobs	Restituisce i dettagli di tutti i lavori. Senza alcun ordine di ordinamento, l'ultimo oggetto Job inviato viene restituito per primo.
server di gestione	OTTENERE	/management-server/jobs/{key} Immettere la chiave di lavoro dell'oggetto Lavoro per visualizzare i dettagli specifici di quel lavoro.	Restituisce i dettagli dell'oggetto Job specifico.

Visualizza i dettagli del sistema

Utilizzando il `/management-server/system` API, puoi interrogare i dettagli specifici dell'istanza del tuo ambiente Unified Manager. L'API restituisce informazioni sul prodotto e sui servizi, come la versione di Unified Manager installata sul sistema, l'UUID, il nome del fornitore, il sistema operativo host e il nome, la descrizione e lo stato dei servizi in esecuzione sull'istanza di Unified Manager.

Categoria	Verbo HTTP	Sentiero	Descrizione
server di gestione	OTTENERE	/management-server/system	Per eseguire questa API non è richiesto alcun parametro di input. Per impostazione predefinita vengono restituiti i dettagli di sistema dell'istanza corrente di Unified Manager.

Gestisci eventi e avvisi tramite API

IL `events`, `alerts`, E `scripts` API sotto il `management-server` La categoria consente di gestire gli eventi, gli avvisi e gli script associati agli avvisi nel tuo ambiente Active IQ Unified Manager .

Visualizza e modifica gli eventi

Unified Manager riceve gli eventi generati su ONTAP per i cluster monitorati e gestiti da Unified Manager. Utilizzando queste API, puoi visualizzare gli eventi generati per i tuoi cluster, risolverli e aggiornarli.

Eseguendo il `GET` metodo per la `/management-server/events` API, puoi interrogare gli eventi nel tuo data center, inclusi i dati storici. Utilizzare i filtri integrati, quali nome, livello di impatto, area di impatto, gravità, stato, nome della risorsa e tipo di risorsa, per visualizzare eventi specifici. I parametri tipo di risorsa e area restituiscono informazioni sull'oggetto di archiviazione su cui si è verificato l'evento, mentre l'area di impatto restituisce informazioni sul problema per cui è stato generato l'evento, ad esempio disponibilità, capacità,

configurazione, sicurezza, protezione e prestazioni.

Eseguendo l'operazione PATCH per questa API, è possibile abilitare il flusso di lavoro di risoluzione per l'evento. Puoi assegnare un evento a te stesso o a un altro utente e confermare la ricezione dell'evento. Dopo aver eseguito i passaggi sulle risorse per risolvere il problema che ha attivato l'evento, puoi utilizzare questa API per contrassegnare l'evento come risolto.

Per maggiori informazioni sugli eventi, vedere ["Gestire gli eventi"](#) .

Categoria	Verbo HTTP	Sentiero	Descrizione
server di gestione	OTTENERE	/management-server/events /management-server/events/{key}	Quando si esegue il metodo Get ALL, il corpo della risposta è costituito dai dettagli di tutti gli eventi nel data center. Quando si recuperano i dettagli dell'evento tramite una chiave specifica, è possibile visualizzare i dettagli di un evento specifico ed eseguire il set successivo di operazioni sulle risorse. Il corpo della risposta è costituito dai dettagli di quell'evento.
server di gestione	TOPPA	management-server/events/{key}	Esegui questa API per assegnare un evento o modificare lo stato in riconosciuto o risolto. Puoi usare questo metodo anche per assegnare l'evento a te stesso o a un altro utente. Si tratta di un'operazione sincrona.

Gestisci gli 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 il /management-server/alerts API, è possibile configurare gli avvisi per inviare notifiche automatiche quando si verificano eventi specifici o eventi di determinati tipi di gravità.

Per ulteriori informazioni sugli avvisi, vedere ["Gestisci gli avvisi"](#) .

Categoria	Verbo HTTP	Sentiero	Descrizione
server di gestione	OTTENERE	/management-server/alerts /management-server/alerts/{key}	Interroga tutti gli avvisi esistenti nel tuo ambiente o un avviso specifico, utilizzando la chiave di avviso. È possibile visualizzare le informazioni sugli avvisi generati nel proprio 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	INVIARE	/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 abilitato 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 dell'e-mail di notifica, i dettagli dello script, nel caso in cui si stia aggiungendo uno script di avviso, e così via.
server di gestione	PATCH e DELETE	management-server/events/{key}	È possibile utilizzare questi metodi per modificare ed eliminare avvisi specifici. È possibile modificare diversi attributi, come la descrizione, il nome e l'attivazione e disattivazione dell'avviso. È possibile eliminare un avviso quando non è più necessario.



Quando si seleziona una risorsa per aggiungere un avviso, tenere presente che la selezione di un cluster come risorsa non comporta la selezione automatica degli oggetti di archiviazione 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.

Gestisci gli script

Utilizzando il `/management-server/scripts` API, è anche possibile associare un avviso a uno script che viene eseguito quando viene attivato un avviso. È possibile utilizzare gli script per modificare o aggiornare automaticamente più oggetti di archiviazione 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 ["Gestisci gli script"](#).

Categoria	Verbo HTTP	Sentiero	Descrizione
server di gestione	OTTENERE	<code>/management-server/scripts</code>	Utilizza questa API per interrogare tutti gli script esistenti nel tuo ambiente. Utilizzare il filtro standard e ordinare per operazioni per visualizzare solo script specifici.
server di gestione	INVIARE	<code>/management-server/scripts</code>	Utilizzare questa API per aggiungere una descrizione per lo script e caricare il file di script associato a un avviso.

Gestisci i carichi di lavoro utilizzando le API

Le API descritte qui coprono varie funzioni di amministrazione dello storage, come la visualizzazione dei carichi di lavoro di storage, la creazione di LUN e condivisioni di file, la gestione dei livelli di servizio delle prestazioni e delle policy di efficienza dello storage e l'assegnazione delle policy sui carichi di lavoro di storage.

Visualizza i carichi di lavoro di archiviazione tramite API

Le API elencate qui consentono di visualizzare un elenco consolidato dei carichi di lavoro di archiviazione per tutti i cluster ONTAP nel data center. Le API forniscono anche una vista riepilogativa del numero di carichi di lavoro di archiviazione forniti nell'ambiente Active IQ Unified Manager e delle relative statistiche di capacità e prestazioni (IOPS).

Visualizza i carichi di lavoro di archiviazione

È possibile utilizzare il metodo seguente per visualizzare tutti i carichi di lavoro di archiviazione in tutti i cluster

del data center. Per informazioni sul filtraggio della risposta in base a colonne specifiche, consulta la documentazione di riferimento API disponibile nella tua istanza di Unified Manager.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/workloads

Visualizza il riepilogo dei carichi di lavoro di archiviazione

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 di archiviazione gestiti da ciascun livello di servizio delle prestazioni. I carichi di lavoro di archiviazione visualizzati possono riguardare qualsiasi LUN, condivisione file NFS o condivisione CIFS. L'API fornisce una panoramica dei carichi di lavoro di storage, una panoramica dei carichi di lavoro di 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 servizio delle prestazioni assegnati. Le informazioni ricevute in risposta a questa API vengono utilizzate per popolare la dashboard nell'interfaccia utente di Unified Manager.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/workloads-summary

Gestisci gli endpoint di accesso utilizzando le API

È necessario creare endpoint di accesso o interfacce logiche (LIF), necessari per il provisioning di macchine virtuali di archiviazione (SVM), LUN e condivisioni file. È possibile visualizzare, creare, modificare ed eliminare gli endpoint di accesso per le SVM, le LUN o le condivisioni file nell'ambiente Active IQ Unified Manager .

Visualizza gli endpoint di accesso

È possibile visualizzare un elenco degli endpoint di accesso nell'ambiente Unified Manager utilizzando il metodo seguente. Per interrogare un elenco di endpoint di accesso di un particolare SVM, LUN o condivisione file, è necessario immettere l'identificatore univoco per l'SVM, la LUN o la condivisione file. È anche possibile immettere la chiave univoca dell'endpoint di accesso per recuperare i dettagli di un determinato endpoint di accesso.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

Aggiungi endpoint di accesso

È possibile creare endpoint di accesso personalizzati e assegnare loro le proprietà richieste. È necessario

immettere i dettagli dell'endpoint di accesso che si desidera creare come parametri di input. È possibile utilizzare questa API, oppure System Manager o ONTAP CLI per creare un endpoint di accesso su ciascun nodo. Per la creazione degli endpoint di accesso sono supportati sia gli indirizzi IPv4 che IPv6.



Per un provisioning corretto di LUN e condivisioni file, è necessario configurare l'SVM con un numero minimo di endpoint di accesso per nodo. Dovresti configurare la tua SVM con almeno due endpoint di accesso per nodo, uno che supporti il protocollo CIFS e/o NFS, l'altro che supporti il protocollo iSCSI o FCP.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/access-endpoints

Elimina gli endpoint di accesso

È possibile eliminare uno specifico endpoint di accesso utilizzando il metodo seguente. Per eliminare un determinato endpoint di accesso, è necessario fornire la chiave dell'endpoint di accesso come parametro di input.

Categoria	Verbo HTTP	Sentiero
fornitore 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 metodo seguente. Per modificare un determinato endpoint di accesso è necessario fornire la chiave dell'endpoint di accesso. È inoltre necessario inserire la proprietà che si desidera aggiornare, insieme al suo valore.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	TOPPA	/storage-provider/access-endpoints/{key}

Gestire la mappatura di Active Directory utilizzando le API

È possibile utilizzare le API elencate qui per gestire i mapping di Active Directory sull'SVM necessari per il provisioning delle condivisioni CIFS sugli SVM. È necessario configurare i mapping di Active Directory per il mapping degli SVM con ONTAP.

Visualizza i mapping di Active Directory

È possibile visualizzare i dettagli di configurazione dei mapping di Active Directory per una SVM utilizzando il metodo seguente. Per visualizzare i mapping di Active Directory su una SVM, è necessario immettere la chiave SVM. Per interrogare i dettagli di una particolare mappatura, è necessario immettere la chiave di mappatura.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/active-directories-mappings /storage-provider/active-directories-mappings/{key}

Aggiungi il mapping di Active Directory

È possibile creare mapping di Active Directory su una SVM utilizzando il metodo seguente. È necessario immettere i dettagli della mappatura come parametri di input.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/active-directories-mappings

Gestisci le condivisioni di file tramite API

Puoi usare il `/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 effettuare il provisioning dei volumi di condivisione file, assicurarsi che l'SVM sia stato creato e predisposto con i protocolli supportati. Se si assegnano livelli di servizio delle prestazioni (PSL) o criteri di efficienza dell'archiviazione (SEP), durante il provisioning, i PSL o gli SEP devono essere creati prima di creare le condivisioni file.

Visualizza le condivisioni di file

È possibile utilizzare il metodo seguente per visualizzare i volumi di condivisione file disponibili nell'ambiente Unified Manager. Dopo aver aggiunto un cluster ONTAP come origine dati su Active IQ Unified Manager, i carichi di lavoro di archiviazione per tali cluster vengono aggiunti automaticamente all'istanza di Unified Manager. Questa API recupera automaticamente e manualmente le condivisioni file aggiunte alla tua istanza di Unified Manager. È possibile visualizzare i dettagli di una specifica condivisione file eseguendo questa API con la chiave di condivisione file.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/file-shares /storage-provider/file-shares/{key}

Aggiungi condivisioni di file

È possibile utilizzare il seguente metodo per aggiungere condivisioni file CIFS e NFS nella propria SVM. È necessario 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	Sentiero
fornitore di storage	INVIARE	/storage-provider/file-shares



A seconda che vengano forniti i parametri dell'elenco di controllo di accesso (ACL) o i parametri della policy di esportazione, vengono create condivisioni CIFS o condivisioni file NFS. Se non si specificano i valori per i parametri ACL, le condivisioni CIFS non vengono create e per impostazione predefinita vengono create le condivisioni NFS, consentendo l'accesso a tutti.

Creazione di volumi di protezione dati: quando si aggiungono condivisioni file al proprio 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 il `type` parametro.

Elimina le condivisioni di file

Per eliminare una condivisione file specifica, è possibile utilizzare il seguente metodo. Per eliminare una determinata condivisione file, è necessario immettere la chiave di condivisione file come parametro di input.

Categoria	Verbo HTTP	Sentiero
fornitore 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.

Per modificare una determinata condivisione file è necessario fornire la chiave di condivisione file. Inoltre, è necessario inserire la proprietà che si desidera aggiornare, insieme al suo valore.



Tieni presente che puoi aggiornare solo una proprietà in una singola invocazione di questa API. Per effettuare più aggiornamenti, è necessario eseguire questa API tante volte.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	TOPPA	/storage-provider/file-shares/{key}

Gestire le LUN utilizzando le API

Puoi usare il `/storage-provider/luns` API per visualizzare, aggiungere, modificare ed eliminare i LUN nel tuo ambiente data center.

Prima di effettuare il provisioning delle LUN, assicurarsi che l'SVM sia stato creato e predisposto con i protocolli supportati. Se si assegnano livelli di servizio delle prestazioni (PSL) o criteri di efficienza dell'archiviazione (SEP), durante il provisioning, i PSL o gli SEP devono essere creati prima di creare la LUN.

Visualizza LUN

È possibile utilizzare il metodo seguente per visualizzare i LUN nell'ambiente Unified Manager. Dopo aver aggiunto un cluster ONTAP come origine dati su Active IQ Unified Manager, i carichi di lavoro di archiviazione per tali cluster vengono aggiunti automaticamente all'istanza di Unified Manager. Questa API recupera automaticamente e manualmente tutti i LUN aggiunti alla tua istanza di Unified Manager. È possibile visualizzare i dettagli di un LUN specifico eseguendo questa API con la chiave LUN.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/luns /storage-provider/luns/{key}

Aggiungi LUN

È possibile utilizzare il seguente metodo per aggiungere LUN alle SVM.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/luns



Nella richiesta cURL, se si fornisce un valore per il parametro facoltativo `volume_name_tag` nell'input, tale valore verrà utilizzato durante la denominazione del volume durante la creazione della LUN. Questo tag consente di cercare facilmente nel volume. Se nella richiesta si specifica la chiave del volume, il tagging verrà ignorato.

Elimina LUN

Per eliminare un LUN specifico è possibile utilizzare il seguente metodo. Per eliminare un LUN specifico è necessario fornire la chiave LUN.



Se hai creato un volume in ONTAP e poi hai eseguito il provisioning delle LUN tramite Unified Manager su quel volume, quando elimini tutte le LUN utilizzando questa API, il volume verrà eliminato anche dal cluster ONTAP.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	ELIMINARE	/storage-provider/luns/{key}

Modificare i LUN

È possibile utilizzare il metodo seguente per modificare una LUN e aggiornarne le proprietà. Per modificare un LUN specifico 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, è necessario consultare i consigli in "Consigli per l'utilizzo delle API".



È possibile aggiornare solo una proprietà in una singola invocazione di questa API. Per effettuare più aggiornamenti, è necessario eseguire questa API tante volte.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	TOPPA	/storage-provider/luns/{key}

Gestire i livelli di servizio delle prestazioni utilizzando le API

È possibile visualizzare, creare, modificare ed eliminare i livelli di servizio delle prestazioni utilizzando le API del provider di archiviazione su Active IQ Unified Manager.

Visualizza i livelli di servizio delle prestazioni

È possibile utilizzare il metodo seguente per visualizzare i livelli di servizio delle prestazioni e assegnarli ai carichi di lavoro di archiviazione. L'API elenca tutti i livelli di servizio delle prestazioni definiti dal sistema e creati dall'utente e recupera gli attributi di tutti i livelli di servizio delle prestazioni. Se si desidera interrogare uno specifico Performance Service Level, è necessario immettere l'ID univoco del Performance Service Level per recuperarne i dettagli.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/performance-service-levels
		/storage-provider/performance-service-levels/{key}

Aggiungi livelli di servizio delle prestazioni

È possibile utilizzare il seguente metodo per creare livelli di servizio delle prestazioni personalizzati e assegnarli ai carichi di lavoro di archiviazione se i livelli di servizio delle prestazioni definiti dal sistema non soddisfano gli obiettivi di livello di servizio (SLO) richiesti per i carichi di lavoro di archiviazione. Inserisci i dettagli per il livello di servizio delle prestazioni che desideri creare. Per le proprietà IOPS, assicurarsi di immettere un intervallo di valori valido.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/performance-service-levels

Elimina i livelli di servizio delle prestazioni

È possibile utilizzare il seguente metodo per eliminare uno specifico livello di servizio delle prestazioni. Non è possibile eliminare un Performance Service Level se è assegnato a un carico di lavoro o se è l'unico Performance Service Level disponibile. Per eliminare un determinato livello di servizio delle prestazioni, è

necessario fornire l'ID univoco del livello di servizio delle prestazioni come parametro di input.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	ELIMINARE	/storage-provider/performance-service-levels/{key}

Modifica i livelli di servizio delle prestazioni

È possibile utilizzare il metodo seguente 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. È necessario fornire l'ID univoco per modificare un determinato livello di servizio delle prestazioni. È inoltre necessario immettere la proprietà IOPS che si desidera aggiornare, insieme a un valore valido.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	TOPPA	/storage-provider/performance-service-levels/{key}

Visualizza le capacità aggregate in base ai livelli di servizio delle prestazioni

È possibile utilizzare il metodo seguente per interrogare le capacità aggregate in base ai livelli di servizio delle prestazioni. Questa API restituisce l'elenco degli aggregati disponibili nel tuo data center e indica le capacità in termini di livelli di servizio delle prestazioni 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 particolare livello di servizio delle prestazioni e di eseguire il provisioning dei carichi di lavoro in base a tale capacità. La possibilità di specificare l'aggregato è disponibile solo quando si esegue il provisioning di un carico di lavoro tramite API. Questa funzionalità non è disponibile nell'interfaccia utente Web di Unified Manager.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/aggregate-capabilities /storage-provider/aggregate-capabilities/{key}

Gestire le policy di efficienza dello storage utilizzando le API

È possibile visualizzare, creare, modificare ed eliminare i criteri di efficienza dell'archiviazione utilizzando le API del provider di archiviazione.

Si prega di notare i seguenti punti:



- Non è obbligatorio assegnare una policy di efficienza dell'archiviazione durante la creazione di un carico di lavoro su Unified Manager.
- Non è possibile annullare l'assegnazione di un criterio di efficienza di archiviazione a un carico di lavoro dopo che gli è stato assegnato un criterio.
- Se un carico di lavoro presenta alcune impostazioni di archiviazione specificate sui volumi ONTAP , come la deduplicazione e la compressione, tali impostazioni possono essere sovrascritte dalle impostazioni specificate nei criteri di efficienza dell'archiviazione applicati quando si aggiungono i carichi di lavoro di archiviazione su Unified Manager.

Visualizza le policy di efficienza di archiviazione

È possibile utilizzare il metodo seguente per visualizzare i criteri di efficienza dell'archiviazione prima di assegnarli ai carichi di lavoro di archiviazione. Questa API elenca tutte le policy di efficienza di archiviazione definite dal sistema e create dall'utente e recupera gli attributi di tutte le policy di efficienza di archiviazione. Se si desidera interrogare una specifica politica di efficienza di archiviazione, è necessario immettere l'ID univoco della politica per recuperarne i dettagli.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/storage-efficiency-policies /storage-provider/storage-efficiency-policies/{key}

Aggiungi criteri di efficienza di archiviazione

È possibile utilizzare il metodo seguente per creare criteri di efficienza di archiviazione personalizzati e assegnarli ai carichi di lavoro di archiviazione se i criteri definiti dal sistema non soddisfano i requisiti di provisioning per i carichi di lavoro di archiviazione. Immettere i dettagli della politica di efficienza di archiviazione che si desidera creare come parametri di input.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/storage-efficiency-policies

Elimina i criteri di efficienza dell'archiviazione

È possibile utilizzare il seguente metodo per eliminare uno specifico criterio di efficienza di archiviazione. Non è possibile eliminare un criterio di efficienza di archiviazione se è assegnato a un carico di lavoro o se è l'unico criterio di efficienza di archiviazione disponibile. Per eliminare una determinata Policy di efficienza di archiviazione, è necessario fornire l'ID univoco della Policy di efficienza di archiviazione come parametro di input.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	ELIMINARE	/storage-provider/storage-efficiency-policies/{key}

Modificare le policy di efficienza di archiviazione

È possibile utilizzare il metodo seguente per modificare un criterio di efficienza di archiviazione e aggiornarne le proprietà. Non è possibile modificare un criterio di efficienza dell'archiviazione definito dal sistema o assegnato a un carico di lavoro. Per modificare una determinata politica di efficienza di archiviazione, è necessario fornire l'ID univoco della politica di efficienza di archiviazione. Inoltre, è necessario fornire l'immobile che si desidera aggiornare, insieme al suo valore.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	TOPPA	/storage-provider/storage-efficiency-policies/{key}

Flussi di lavoro API comuni per la gestione dell'archiviazione

I flussi di lavoro comuni forniscono agli sviluppatori di applicazioni client esempi di come le API di Active IQ Unified Manager possono essere richiamate da un'applicazione client per eseguire funzioni comuni di gestione dell'archiviazione. Questa sezione contiene alcuni di questi flussi di lavoro di esempio.

I flussi di lavoro descrivono alcuni dei casi d'uso più comuni per la gestione dell'archiviazione, insieme a codici di esempio da utilizzare. Ciascuna attività viene descritta mediante un processo di flusso di lavoro costituito da una o più chiamate API.

Comprendere le chiamate API utilizzate nei flussi di lavoro

È possibile visualizzare la pagina della documentazione online dalla propria istanza di Unified Manager, che include i dettagli di ogni chiamata API REST. Il presente documento non ripete i dettagli della documentazione online. Ogni chiamata API utilizzata negli esempi di flusso di lavoro in questo documento include solo le informazioni necessarie per individuare la chiamata nella pagina della documentazione. Dopo aver individuato una specifica chiamata API, è possibile esaminarne i dettagli completi, inclusi i parametri di input, i formati di output, i codici di stato HTTP e il tipo di elaborazione della richiesta.

Per ogni chiamata API all'interno di un flusso di lavoro sono incluse le seguenti informazioni, che aiutano a individuare la chiamata nella pagina della documentazione:

- **Categoria:** le chiamate API sono organizzate nella pagina della documentazione in aree o categorie funzionalmente correlate. Per individuare una chiamata API specifica, scorrere fino alla fine della pagina e 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 si applica l'azione 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.

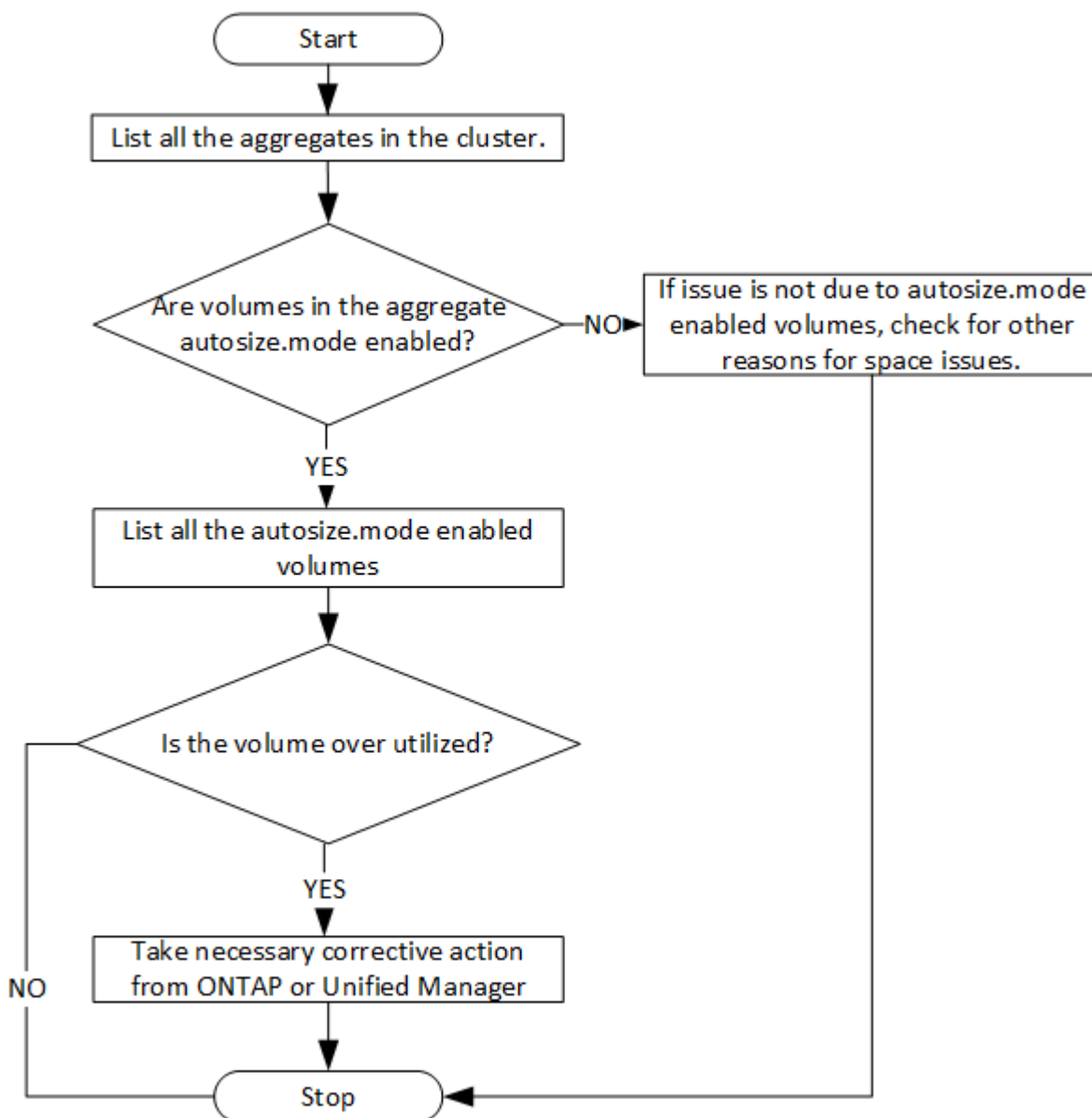
Determinare i problemi di spazio negli aggregati utilizzando le API

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 archiviazione sovrautilizzate o sottoutilizzate.

Le API del data center per gli aggregati recuperano le informazioni rilevanti sullo spazio disponibile e utilizzato, nonché sulle impostazioni di efficienza del risparmio di spazio. È anche possibile filtrare le informazioni recuperate in base ad attributi specifici.

Un metodo per determinare la mancanza di spazio negli aggregati è verificare se nell'ambiente sono presenti volumi con la modalità autosize abilitata. Dovresti quindi identificare quali volumi sono sovrautilizzati ed eseguire eventuali azioni correttive.

Il seguente diagramma di flusso illustra il processo di recupero delle informazioni sui volumi con la modalità autosize abilitata:



Questo flusso presuppone che i cluster siano già stati creati in ONTAP e aggiunti a Unified Manager.

1. Ottieni la chiave del cluster, a meno che tu non conosca il valore:

Categoria	Verbo HTTP	Sentiero
centro dati	OTTENERE	/datacenter/cluster/clusters

2. Utilizzando la chiave del cluster come parametro di filtro, interrogare gli aggregati su quel cluster.

Categoria	Verbo HTTP	Sentiero
centro dati	OTTENERE	/datacenter/storage/aggregates

3. In base alla risposta, analizzare l'utilizzo dello spazio degli aggregati e determinare 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 che hanno il valore per il parametro `autosize.mode` come `grow`.

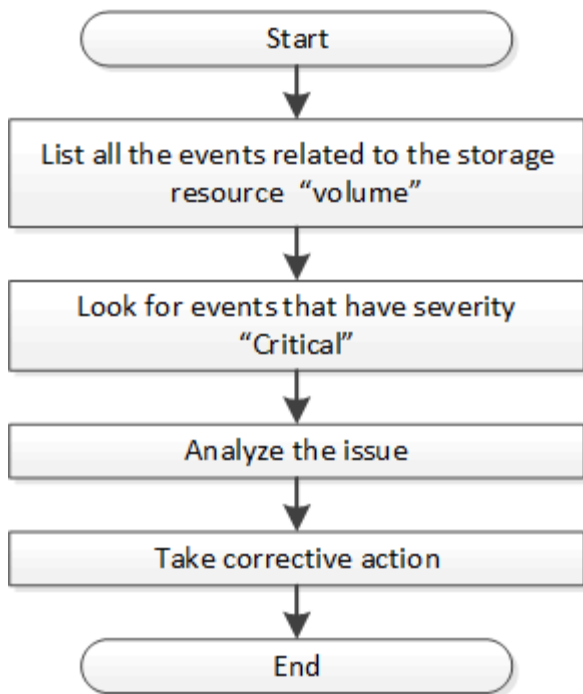
Categoria	Verbo HTTP	Sentiero
centro dati	OTTENERE	/datacenter/storage/volumes

5. Analizzare quali volumi sono sovrautilizzati.
6. Eseguire tutte le azioni correttive necessarie, come lo spostamento del volume tra gli aggregati, per risolvere i problemi di spazio nel volume. È possibile eseguire queste azioni dall'interfaccia utente Web di ONTAP o Unified Manager.

Determinare i problemi negli oggetti di archiviazione utilizzando le API degli eventi

Quando un oggetto di archiviazione nel tuo data center supera una soglia, ricevi una notifica relativa a tale evento. Utilizzando questa notifica, è possibile analizzare il problema e adottare misure correttive utilizzando `events` API.

Questo flusso di lavoro prende come esempio un volume come oggetto risorsa. Puoi usare il `events` API per recuperare l'elenco degli eventi correlati a un volume, analizzare i problemi critici per quel volume e quindi intraprendere azioni correttive per risolvere il problema.



Seguire questi passaggi per individuare i problemi nel volume prima di adottare misure correttive.

Passi

1. Analizza le notifiche degli eventi critici Active IQ Unified Manager per i volumi nel tuo data center.
2. Interrogare tutti gli eventi per i volumi utilizzando i seguenti parametri nell'API /management-server/events:
"resource_type": "volume"
"severity": "critical"

Categoria	Verbo HTTP	Sentiero
server di gestione	OTTENERE	/server-di-gestione/eventi

3. Visualizza l'output e analizza 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.

Risolvere i problemi dei volumi ONTAP utilizzando le API del gateway

Le API gateway fungono da gateway per richiamare le API ONTAP per interrogare informazioni sugli oggetti di archiviazione ONTAP e adottare misure correttive per risolvere i problemi segnalati.

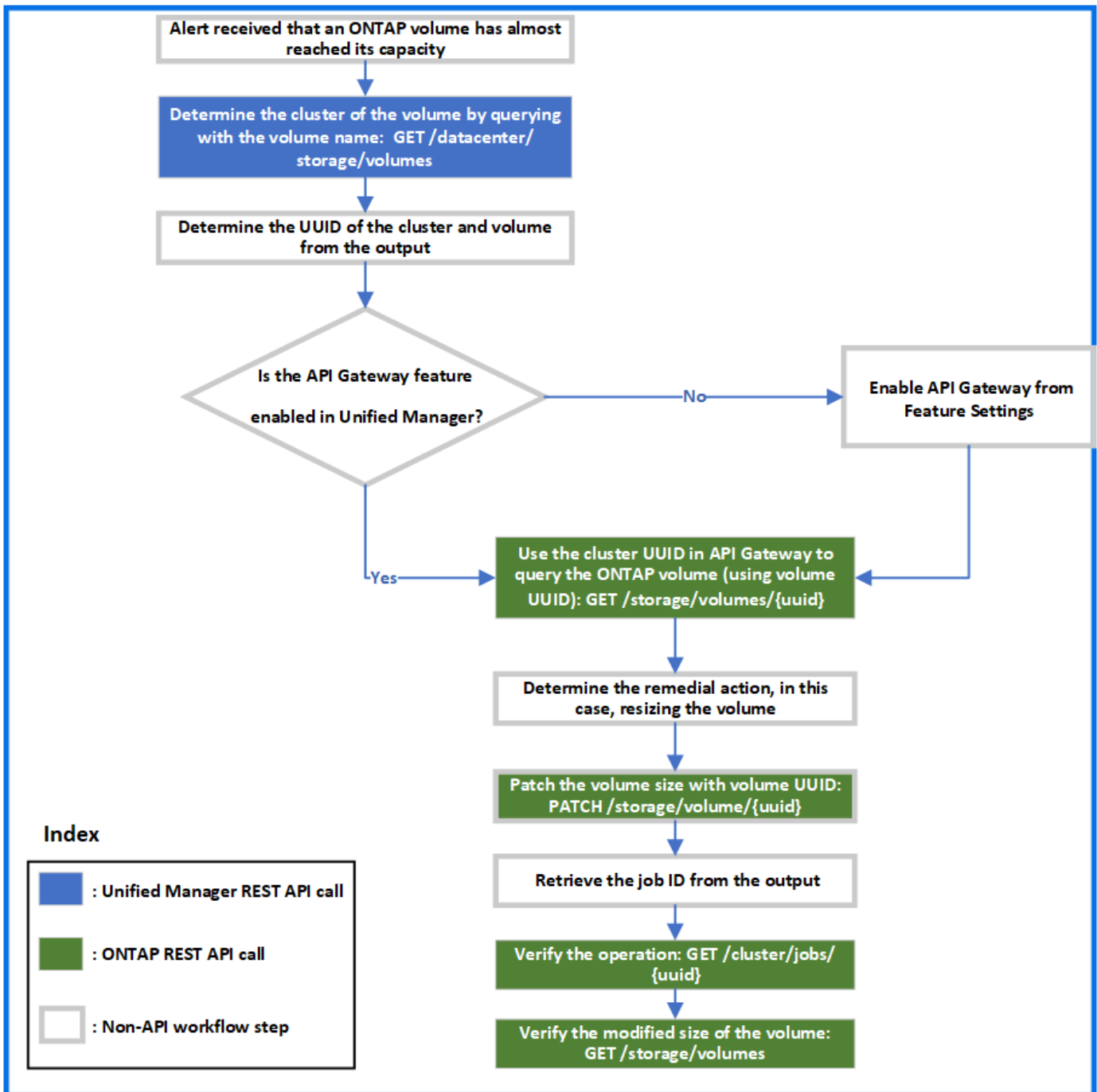
Questo flusso di lavoro riprende un caso d'uso di esempio in cui viene generato un evento quando un volume ONTAP raggiunge quasi la sua capacità. Il flusso di lavoro illustra anche come risolvere questo problema richiamando una combinazione di Active IQ Unified Manager e API REST ONTAP .

Prima di eseguire i passaggi del flusso di lavoro, assicurarsi di quanto segue:



- Conosci le API del gateway e il modo in cui vengono utilizzate. Per informazioni, vedere ["Accesso alle API ONTAP tramite accesso proxy"](#) .
- Sei a conoscenza dell'utilizzo delle API REST ONTAP . Per informazioni sull'utilizzo delle API REST ONTAP , vedere <https://docs.netapp.com/us-en/ontap-automation/index.html> ["Documentazione di automazione ONTAP"] .
- Sei un amministratore dell'applicazione.
- Il cluster su cui si desidera eseguire le operazioni REST API è supportato da ONTAP 9.5 o versione successiva e il cluster viene aggiunto a Unified Manager tramite HTTPS.

Il diagramma seguente illustra ogni passaggio 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 invocazione delle API REST di Unified Manager e ONTAP .

1. Annotare il nome del volume dall'evento che notifica l'utilizzo della capacità del volume.
2. Utilizzando il nome del volume come valore nel parametro name, interrogare il volume eseguendo la seguente API Unified Manager.

Categoria	Verbo HTTP	Sentiero
centro dati	OTTENERE	/datacenter/storage/volumes

3. Recupera l'UUID del cluster e l'UUID del volume dall'output.

4. Nell'interfaccia utente Web di Unified Manager, vai su **Generale > Impostazioni funzionalità > API Gateway** per verificare se la funzionalità API Gateway è abilitata. Se non è abilitata, le API nella categoria gateway non possono essere richiamate. Abilitare la funzione se è disabilitata.
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 eseguire le API ONTAP tramite API Gateway, le credenziali di Unified Manager vengono passate internamente per l'autenticazione e non è necessario eseguire un ulteriore passaggio di autenticazione per l'accesso al cluster individuale.

Categoria	Verbo HTTP	Sentiero
Unified Manager: gateway ONTAP: archiviazione	OTTENERE	API del gateway: /gateways/{uuid}/{path} API ONTAP : /storage/volumes/{uuid}



In /gateways/{uuid}/{path}, il valore per {uuid} deve essere sostituito con l'UUID del cluster su cui deve essere eseguita l'operazione REST. {path} deve essere sostituito dall'URL REST ONTAP /storage/volumes/{uuid}.

L'URL aggiunto è: /gateways/{cluster_uuid}/storage/volumes/{volume_uuid}

Eseguendo l'operazione GET, l'URL generato è:

GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}

Esempio di comando cURL

```
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. In base all'output, determinare le dimensioni, l'utilizzo e le misure correttive da adottare. In questo flusso di lavoro, la misura correttiva adottata è il ridimensionamento del volume.
7. Utilizzare l'UUID del cluster ed eseguire la seguente API ONTAP tramite 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	Sentiero
Unified Manager: gateway ONTAP: archiviazione	TOPPA	API del gateway: /gateways/{uuid}/{path} API ONTAP : /storage/volumes/{uuid}



Oltre all'UUID del cluster e all'UUID del volume, è necessario immettere un valore per il parametro size per ridimensionare il 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, immettere il valore per il parametro size alla fine della query: `-d {"size": 128849018880}`

Esempio di comando cURL

```
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 processo.

- 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 tramite il gateway API. Per informazioni sui parametri di input per il gateway e le API ONTAP, vedere il passaggio 5.

Categoria	Verbo HTTP	Sentiero
Unified Manager: gateway ONTAP: cluster	OTTENERE	API del gateway: /gateways/{uuid}/{path} API ONTAP : /cluster/jobs/{uuid}

I codici HTTP restituiti sono gli stessi codici di stato HTTP dell'API REST ONTAP .

- Eseguire la seguente API ONTAP per interrogare i dettagli del volume ridimensionato. Per informazioni sui parametri di input per il gateway e le API ONTAP, vedere il passaggio 5.

Categoria	Verbo HTTP	Sentiero
Unified Manager: gateway ONTAP: archiviazione	OTTENERE	API del gateway: /gateways/{uuid}/{path} API ONTAP : /storage/volumes/{uuid}

L'output mostra un volume aumentato di 120 GB.

Flussi di lavoro API per la gestione del carico di lavoro

Utilizzando Active IQ Unified Manager, è possibile effettuare il provisioning e modificare i carichi di lavoro di archiviazione (LUN, condivisioni file NFS e condivisioni CIFS). Il provisioning è costituito da più passaggi, dalla creazione della Storage Virtual Machine

(SVM) all'applicazione dei criteri di efficienza dello storage e del livello di servizio delle prestazioni sui carichi di lavoro di storage. La modifica dei carichi di lavoro consiste nei passaggi per modificare parametri specifici e abilitare funzionalità aggiuntive su di essi.

Vengono descritti i seguenti flussi di lavoro:

- Flusso di lavoro per il provisioning di macchine virtuali di archiviazione (SVM) su Unified Manager.



questo flusso di lavoro deve essere eseguito prima di effettuare il provisioning di LUN o condivisioni file su Unified Manager.

- Provisioning delle condivisioni di file.
- Provisioning delle LUN.
- Modifica di LUN e condivisioni file (utilizzando l'esempio per aggiornare il parametro Performance Service Level per i carichi di lavoro di archiviazione).
- 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 file), assicurati di aver completato il flusso di lavoro per la verifica delle SVM sui cluster.

È inoltre necessario leggere le raccomandazioni e le limitazioni prima di utilizzare ciascuna API nei flussi di lavoro. I dettagli rilevanti delle API sono disponibili nelle singole sezioni elencate nei concetti e nei riferimenti correlati.

Verificare le SVM sui cluster utilizzando le API

Prima di effettuare il provisioning di condivisioni file o LUN, è necessario verificare se sui cluster sono state create macchine virtuali di archiviazione (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 di LUN e condivisioni di file su di essi.

1. Verificare se nel cluster è stata creata una SVM.

Categoria	Verbo HTTP	Sentiero
centro dati	OTTENERE	/datacenter/svm/svms /datacenter/svm/svms/{key }

Esempio di cURL

```
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 l'SVM. Per creare le SVM, è necessaria la chiave del cluster su cui si esegue il provisioning della SVM. È inoltre necessario specificare il nome SVM. Seguire questi passaggi.

Categoria	Verbo HTTP	Sentiero
centro dati	OTTENERE	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

Ottieni la chiave del cluster.

Esempio di cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

3. Dall'output, ricava la chiave del cluster e usala come input per creare l'SVM.



Durante la creazione dell'SVM, assicurarsi che supporti tutti i protocolli richiesti per il provisioning di LUN e condivisioni di file su di essi, ad esempio CIFS, NFS, FCP e iSCSI. I flussi di lavoro di provisioning potrebbero non funzionare se l'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	Sentiero
centro dati	INVIARE	/datacenter/svm/svms

Esempio di cURL

Immettere 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\" ] }, \"fcg\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true, \"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" } }, \"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\": \"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" }, \"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\", \"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\", \"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"name\": \"svm1\", \"nfs\": { \"enabled\": true }, \"nis\": { \"domain\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true }, \"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" }, \"gateway\": \"string\" } ], \"snapshot_policy\": { \"name\": \"default\" }, \"state\": \"running\", \"subtype\": \"default\"}"
```

L'output JSON visualizza una chiave dell'oggetto Job che puoi utilizzare per verificare l'SVM che hai creato.

4. Verificare la creazione dell'SVM utilizzando la chiave dell'oggetto job per la query. Se la SVM viene creata correttamente, la chiave SVM viene restituita nella risposta.

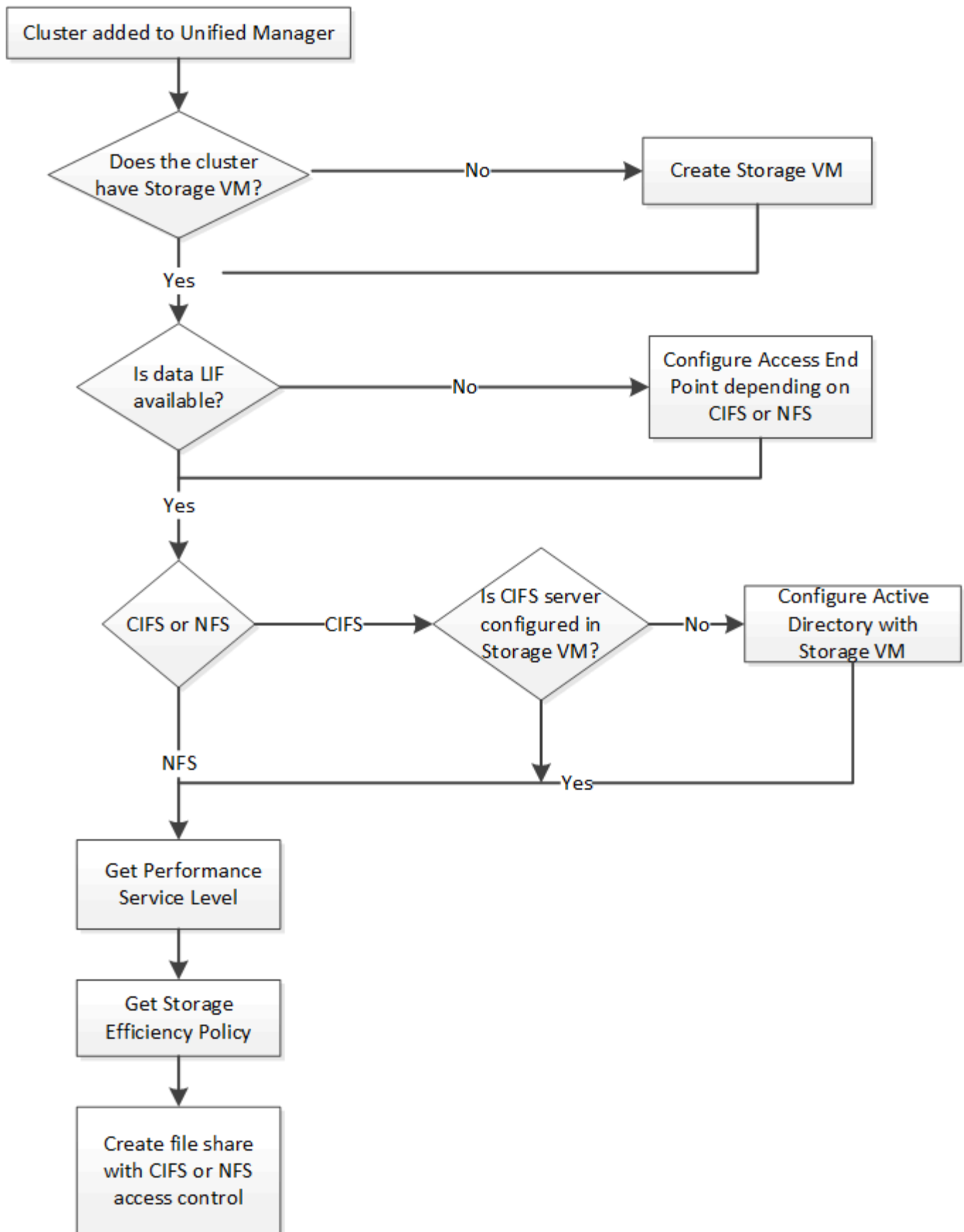
Categoria	Verbo HTTP	Sentiero
server di gestione	OTTENERE	/management-server/jobs/{key}

Fornire condivisioni di file CIFS e NFS utilizzando le API

È possibile effettuare il provisioning di condivisioni CIFS e condivisioni file NFS sulle

macchine virtuali di archiviazione (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 recuperare le chiavi delle SVM, i livelli di servizio delle prestazioni e i criteri di efficienza dell'archiviazione prima di creare le condivisioni file.

Il diagramma seguente illustra ogni passaggio di un flusso di lavoro di provisioning della condivisione file. Include il provisioning sia delle condivisioni CIFS che delle condivisioni file NFS.



Assicurarsi che:



- I cluster ONTAP sono stati aggiunti a Unified Manager ed è stata ottenuta la chiave del cluster.
- Sono state create delle SVM sui cluster.
- Le SVM supportano i servizi CIFS e NFS. Il provisioning delle condivisioni 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 i LIF dati o gli endpoint di accesso sono disponibili sull'SVM su cui si desidera creare la condivisione CIFS. Ottieni l'elenco degli endpoint di accesso disponibili sull'SVM:

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

Esempio di cURL

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. 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 su cui sia abilitato il protocollo CIFS. Il provisioning delle condivisioni CIFS non riesce a meno che non sia stato creato un endpoint di accesso con il protocollo CIFS abilitato.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/access-endpoints

Esempio di cURL

È necessario 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 dell'oggetto Job che puoi utilizzare per verificare l'endpoint di accesso creato.

3. Verificare l'endpoint di accesso:

Categoria	Verbo HTTP	Sentiero
server di gestione	OTTENERE	/management-server/jobs/{key}

4. Determina se devi creare una condivisione CIFS o una condivisione file NFS. Per creare condivisioni CIFS, seguire questi passaggi:

- Determinare se il server CIFS è configurato sulla SVM, ovvero se è stata creata una mappatura di Active Directory sulla SVM.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/active-directories-mappings

- Se il mapping di Active Directory è stato creato, prendere la chiave, altrimenti creare il mapping di Active Directory sull'SVM.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/active-directories-mappings

Esempio di cURL

È necessario immettere 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 di Active Directory nell'output. In caso di errore, viene visualizzato un messaggio di errore per consentirti di risolvere il problema e rieseguire la richiesta.

5. Ottenere la chiave SVM per l'SVM su cui si desidera creare la condivisione CIFS o la condivisione file NFS, come descritto nell'argomento del flusso di lavoro *Verifica delle SVM sui cluster*.
6. Ottieni la chiave per il Performance Service Level eseguendo la seguente API e recuperando la chiave dalla risposta.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/performance-service-levels



È possibile recuperare i dettagli dei livelli di servizio delle prestazioni definiti dal sistema impostando `system_defined` parametro di input a `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare alla condivisione file.

7. Facoltativamente, è possibile 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	Sentiero
fornitore di storage	OTTENERE	/storage-provider/storage-efficiency-policies

8. Crea la condivisione file. È possibile creare una condivisione file che supporti sia CIFS che NFS specificando l'elenco di controllo degli accessi e i criteri di esportazione. I seguenti sotto-passaggi

forniscono informazioni se si desidera creare una condivisione file per supportare solo uno dei protocolli sul volume. È anche possibile aggiornare una condivisione file NFS per includere l'elenco di controllo degli accessi dopo aver creato la condivisione NFS. Per informazioni, vedere l'argomento *Modifica dei carichi di lavoro di archiviazione*.

- a. Per creare solo una condivisione CIFS, raccogliere le informazioni sull'elenco di controllo degli accessi (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 fornita una condivisione CIFS/SMB. In base ai valori immessi per l'ACL e il mapping di Active Directory, il controllo di accesso e il mapping vengono determinati per la condivisione CIFS al momento della sua 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 sulla policy di esportazione. Per creare la condivisione file NFS, fornire valori validi per i seguenti parametri di input. In base ai valori specificati, il criterio di esportazione viene associato alla condivisione file NFS al momento della creazione.



Durante il provisioning della condivisione NFS, è possibile creare un criterio di esportazione specificando tutti i valori richiesti oppure specificare la chiave del criterio di esportazione e riutilizzare un criterio di esportazione esistente. Se si desidera riutilizzare un criterio di esportazione per la VM di archiviazione, è necessario aggiungere la chiave del criterio di esportazione. A meno che non si conosca la chiave, è possibile recuperare la chiave della policy di esportazione utilizzando `/datacenter/protocols/nfs/export-policies` API. Per creare una nuova policy, è necessario immettere le regole come mostrato nell'esempio seguente. Per le regole immesse, l'API tenta di cercare una policy di esportazione esistente confrontando l'host, la VM di archiviazione e le regole. Se esiste una politica di esportazione, questa viene utilizzata. In caso contrario, verrà creata una nuova politica 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 file CIFS e NFS:



Storage Efficiency Policy è un parametro facoltativo per la creazione di condivisioni di file.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/file-shares

L'output JSON visualizza una chiave dell'oggetto Job che puoi utilizzare per verificare la condivisione file creata. . Verificare la creazione della condivisione file utilizzando la chiave dell'oggetto Job restituita durante la query del job:

Categoria	Verbo HTTP	Sentiero
server di gestione	OTTENERE	/management-server/jobs/{key}

Alla fine 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	Sentiero
fornitore di storage	OTTENERE	/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, invoca il /storage-provider/performance-service-levels/ API per l'assegnazione del livello di servizio delle prestazioni sulla 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": [

```

```

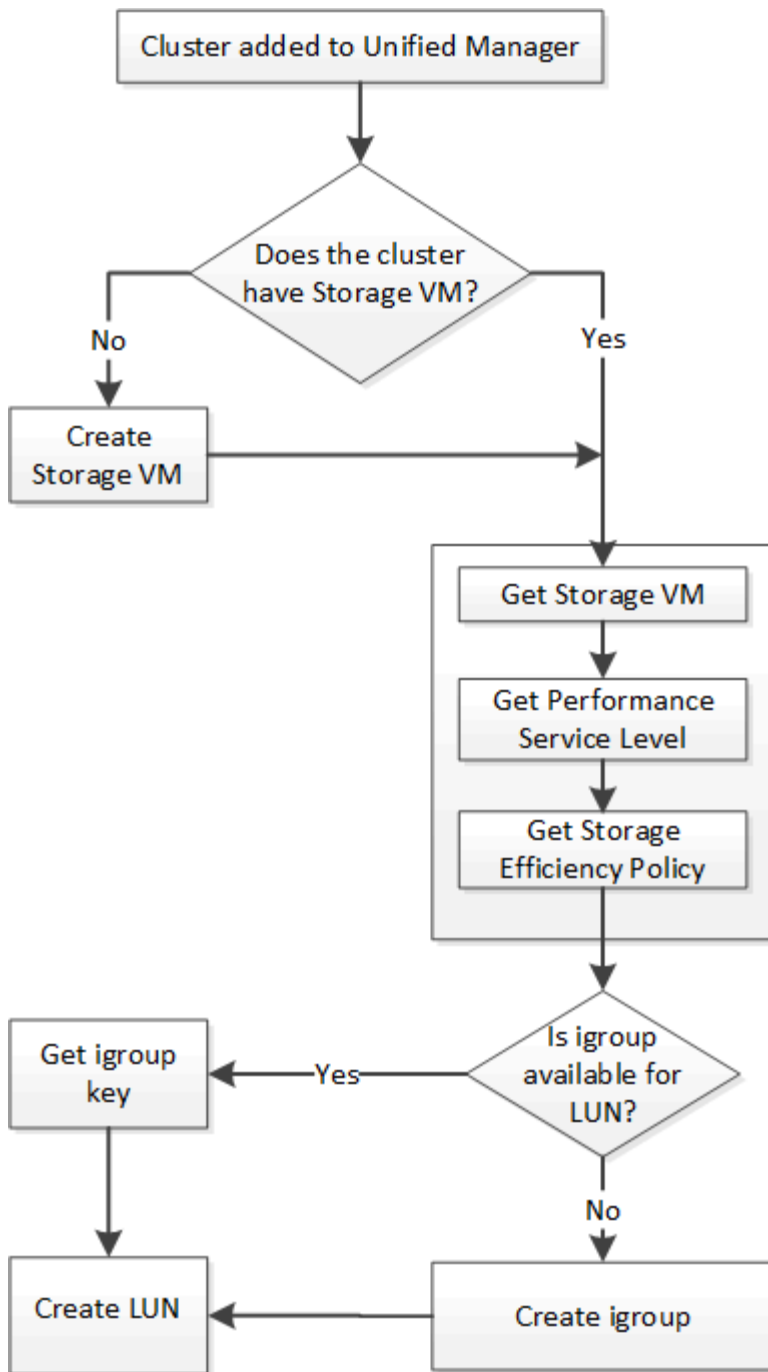
        "ntlm"
    ],
    "superuser": [
        "none"
    ]
}
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}
}

```

Fornire LUN tramite API

È possibile effettuare il provisioning delle LUN sulle macchine virtuali di archiviazione (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 recuperare le chiavi delle SVM, dei livelli di servizio delle prestazioni e dei criteri di efficienza dell'archiviazione prima di creare la LUN.

Il diagramma seguente illustra i passaggi di un flusso di lavoro di provisioning 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 l'SVM su cui si desidera creare la LUN, come descritto nell'argomento del flusso di lavoro *Verifica delle SVM sui cluster*.
2. Ottieni la chiave per il Performance Service Level eseguendo la seguente API e recuperando la chiave dalla risposta.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/performance-service-levels



È possibile recuperare i dettagli dei livelli di servizio delle prestazioni definiti dal sistema impostando `system_defined` parametro di input a `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare alla LUN.

- Facoltativamente, è possibile ottenere la chiave Storage Efficiency Policy per la Storage Efficiency Policy che si desidera applicare alla LUN eseguendo la seguente API e recuperando la chiave dalla risposta.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/storage-efficiency-policies

- Determinare se sono stati creati gruppi di iniziatori (igroup) per concedere l'accesso alla destinazione LUN che si desidera creare.

Categoria	Verbo HTTP	Sentiero
centro dati	OTTENERE	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}

È necessario immettere il valore del parametro per indicare l'SVM per il quale l'igroup ha accesso autorizzato. Inoltre, se si desidera interrogare un particolare igroup, immettere il nome dell'igroup (chiave) come parametro di input.

- Nell'output, se riesci a trovare l'igroup a cui vuoi concedere l'accesso, ottieni la chiave. Altrimenti creare l'igroup.

Categoria	Verbo HTTP	Sentiero
centro dati	INVIARE	/datacenter/protocols/san/igroups

È necessario immettere i dettagli dell'igroup che si desidera creare come parametri di input. Questa è una chiamata sincrona ed è possibile verificare la creazione dell'igroup nell'output. In caso di errore, viene visualizzato un messaggio che consente di risolvere il problema e di rieseguire l'API.

- Creare il LUN.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/luns

Per creare il LUN, assicurarsi di aver aggiunto i valori recuperati come parametri di input obbligatori.



Storage Efficiency Policy è un parametro facoltativo per la creazione di LUN.

Esempio di cURL

È necessario immettere tutti i dettagli della LUN che si desidera creare come parametri di input.

L'output JSON visualizza una chiave dell'oggetto Job che puoi utilizzare per verificare il LUN creato.

7. Verificare la creazione del LUN utilizzando la chiave dell'oggetto Job restituita durante la query del Job:

Categoria	Verbo HTTP	Sentiero
server di gestione	OTTENERE	/management-server/jobs/{key}

Alla fine 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	Sentiero
fornitore di storage	OTTENERE	/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, invoca il `/storage-provider/performance-service-levels/` API per l'assegnazione del livello di servizio delle prestazioni sulla LUN.

== Passaggi per la risoluzione dei problemi in caso di errore nella creazione o nella mappatura LUN

Anche dopo aver completato questo flusso di lavoro, potresti comunque riscontrare un errore nella creazione del LUN. Anche se la LUN viene creata correttamente, il mapping della LUN con l'igroup potrebbe non riuscire a causa della mancata disponibilità di un SAN LIF o di un endpoint di accesso sul nodo su cui si crea la LUN. In caso di errore, verrà 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 questo problema, seguire questi passaggi per la risoluzione dei problemi.

1. Creare un endpoint di accesso che supporti il protocollo iSCSI/FCP sull'SVM su cui si è tentato di creare il LUN.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	INVIARE	/storage-provider/access-endpoints

Esempio di cURL

È necessario immettere i dettagli dell'endpoint di accesso che si desidera creare come parametri di input.



Assicurarsi di aver aggiunto nel parametro di input l'indirizzo per indicare il nodo home della LUN e ha_address per indicare il nodo partner del nodo home. Quando si esegue questa operazione, vengono creati endpoint di accesso sia sul nodo home che sul nodo partner.

2. Eseguire una query sul processo con la chiave dell'oggetto processo restituita nell'output JSON per verificare che sia stato eseguito correttamente per aggiungere gli endpoint di accesso sull'SVM e che i servizi iSCSI/FCP siano stati abilitati sull'SVM.

Categoria	Verbo HTTP	Sentiero
server di gestione	OTTENERE	/management-server/jobs/{key}

Esempio di output JSON

Alla fine dell'output è possibile visualizzare la chiave degli endpoint di accesso creati. Nell'output seguente, il valore "name": "accessEndpointKey" indica l'endpoint di accesso creato sul nodo home della LUN, per il quale la chiave è 9c964258-14ef-11ea-95e2-00a098e32c28. Il valore "name": "accessEndpointHKey" indica l'endpoint di accesso creato sul 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 flusso di lavoro, vedere "Modifica dei carichi di lavoro di archiviazione".

Categoria	Verbo HTTP	Sentiero
fornitore di storage	TOPPA	/storage-provider/lun/{key}

Nell'input, specificare la chiave igroup con cui si desidera aggiornare la mappatura LUN, insieme alla chiave LUN.

Esempio di cURL

L'output JSON visualizza una chiave dell'oggetto Job che è possibile utilizzare per verificare se la mappatura è riuscita.

4. Verificare la mappatura LUN eseguendo una query con la chiave LUN.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/luns/{key}

Esempio di output JSON

Nell'output è possibile vedere che la LUN è stata mappata correttamente con l'igroup (chiave d19ec2fa-fec7-11e8-b23d-00a098e32c28) con cui era stata inizialmente predisposta.

Modificare i carichi di lavoro di archiviazione utilizzando le API

La modifica dei carichi di lavoro di archiviazione consiste nell'aggiornare le LUN o le condivisioni file con parametri mancanti oppure nel modificare i parametri esistenti.

Questo flusso di lavoro prende come esempio l'aggiornamento dei livelli di servizio delle prestazioni per LUN e condivisioni di file.



Il flusso di lavoro presuppone che la LUN o la condivisione file siano state dotate di livelli di servizio di prestazioni.

Modificare le condivisioni di file

Durante la modifica di una condivisione file, è possibile aggiornare i seguenti parametri:

- Capacità o dimensione.
- Impostazione online o offline.
- Politica di efficienza di archiviazione.
- Livello di servizio prestazionale.
- Impostazioni dell'elenco di controllo degli accessi (ACL).
- Esporta le impostazioni dei criteri. È anche possibile eliminare i parametri dei criteri di esportazione e ripristinare le regole predefinite (vuote) dei criteri di esportazione sulla condivisione file.



Durante una singola esecuzione dell'API, è possibile aggiornare solo un parametro.

Questa procedura descrive come aggiungere un livello di servizio delle prestazioni a una condivisione file. È possibile utilizzare la stessa procedura per aggiornare qualsiasi altra proprietà di condivisione file.

1. Ottieni la chiave di condivisione CIFS o di condivisione file NFS della condivisione file che desideri aggiornare. Questa API interroga tutte le condivisioni file sul tuo data center. Salta questo passaggio se conosci già la chiave di condivisione file.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/file-shares

2. Visualizza i dettagli della condivisione file eseguendo la seguente API con la chiave di condivisione file

ottenuta.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/file-shares/{key}

Visualizza i dettagli della condivisione file nell'output.

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. Ottieni la chiave per il livello di servizio delle prestazioni che desideri assegnare a questa condivisione file. Attualmente non gli è assegnata alcuna policy.

Categoria	Verbo HTTP	Sentiero
Livelli di servizio prestazionali	OTTENERE	/storage-provider/performance-service-levels



È possibile recuperare i dettagli dei livelli di servizio delle prestazioni definiti dal sistema impostando `system_defined` parametro di input a `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare alla condivisione file.

4. Applicare il livello di servizio delle prestazioni alla condivisione file.

Categoria	Verbo HTTP	Sentiero
Fornitore di archiviazione	TOPPA	/storage-provider/file-shares/{key}

Nell'input è necessario specificare solo il parametro che si desidera aggiornare, insieme alla chiave di condivisione file. In questo caso, è la chiave del Performance Service Level.

Esempio di cURL

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

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 la chiave dell'oggetto Job visualizzata nell'output.

Categoria	Verbo HTTP	Sentiero
Server di gestione	OTTENERE	/management-server/jobs/{key}

Se si esegue una query tramite l'ID dell'oggetto Job, è possibile verificare se la condivisione file è stata aggiornata correttamente. In caso di errore, risolvere il problema ed eseguire nuovamente l'API. Una volta completata la creazione, interroga la condivisione file per visualizzare l'oggetto modificato:

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/storage-provider/file-shares/{key}

Visualizza 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"
    }
  }
}
```

Aggiorna LUN

Durante l'aggiornamento di una LUN, è possibile modificare i seguenti parametri:

- Capacità o dimensione
- Impostazione online o offline
- Politica di efficienza di archiviazione
- Livello di servizio delle prestazioni
- Mappa LUN



Durante una singola esecuzione dell'API, è possibile aggiornare solo un parametro.

Questa procedura descrive come aggiungere un livello di servizio delle prestazioni a una LUN. È possibile utilizzare la stessa procedura per aggiornare qualsiasi altra proprietà LUN.

1. Ottieni la chiave LUN della LUN che vuoi aggiornare. Questa API restituisce i dettagli di tutti i LUN nel tuo data center. Saltare questo passaggio se si conosce già la chiave LUN.

Categoria	Verbo HTTP	Sentiero
Fornitore di archiviazione	OTTENERE	/storage-provider/luns

2. Visualizza i dettagli del LUN eseguendo la seguente API con la chiave LUN ottenuta.

Categoria	Verbo HTTP	Sentiero
Fornitore di archiviazione	OTTENERE	/storage-provider/luns/{key}

Visualizza i dettagli del LUN nell'output. Come puoi vedere, a questo LUN non è assegnato alcun livello di servizio delle prestazioni.

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 Performance Service Level che si desidera assegnare al LUN.

Categoria	Verbo HTTP	Sentiero
Livelli di servizio prestazionali	OTTENERE	/storage-provider/performance-service-levels



È possibile recuperare i dettagli dei livelli di servizio delle prestazioni definiti dal sistema impostando `system_defined` parametro di input a `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare alla LUN.

4. Applicare il livello di servizio delle prestazioni sulla LUN.

Categoria	Verbo HTTP	Sentiero
Fornitore di archiviazione	TOPPA	/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 Performance Service Level.

Esempio di cURL

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" } }"
```

L'output JSON visualizza una chiave dell'oggetto Job che puoi utilizzare per verificare il LUN che hai aggiornato.

5. Visualizza i dettagli del LUN eseguendo la seguente API con la chiave LUN ottenuta.

Categoria	Verbo HTTP	Sentiero
Fornitore di archiviazione	OTTENERE	/storage-provider/luns/{key}

Visualizza i dettagli del LUN nell'output. È possibile vedere che a questo LUN è assegnato il Performance Service Level.

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"
    }
  }
}

```

Modificare una condivisione file NFS utilizzando le API per supportare CIFS

È possibile modificare una condivisione file NFS per supportare il protocollo CIFS. Durante la creazione della condivisione file, è possibile specificare sia i parametri dell'elenco di controllo degli accessi (ACL) sia le regole dei criteri di esportazione per la stessa condivisione file. Tuttavia, se si desidera abilitare 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.

Prima di iniziare

1. Deve essere stata creata una condivisione file NFS con solo i dettagli della policy di esportazione. Per informazioni, vedere *Gestione delle condivisioni file* e *Modifica dei carichi di lavoro di archiviazione*.
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 tramite l'ID processo, vedere *Provisioning di condivisioni file CIFS e NFS*.

Ciò è applicabile a una condivisione file NFS creata aggiungendo solo regole di policy di esportazione e non parametri ACL. Modificare la condivisione file NFS per includere i parametri ACL.

Passi

1. Sulla condivisione file NFS, eseguire un `PATCH` operazione con i dettagli ACL per consentire l'accesso CIFS.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	TOPPA	/storage-provider/file-shares

Esempio di cURL

In base ai privilegi di accesso assegnati al gruppo 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 del job che esegue l'aggiornamento.

2. Verificare se i parametri sono stati aggiunti correttamente interrogando i dettagli della condivisione file per la stessa condivisione file.

Categoria	Verbo HTTP	Sentiero
fornitore di storage	OTTENERE	/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 alla policy di esportazione sulla stessa condivisione file.

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](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>

Politica sulla riservatezza

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open source

Informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati in questo prodotto.

["Avviso per Active IQ Unified Manager 9.16"](#)

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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.