Documentazione Data Infrastructure Insights

Data Infrastructure Insights

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/it-it/data-infrastructure-insights/index.html on February 11, 2026. Always check docs.netapp.com for the latest.

Sommario

Documentazione Data Infrastructure Insights . . . 1
Cosa può fare per me Data Infrastructure Insights ? . . . 1
Iniziare . . . 1
Novità di Data Infrastructure Insights . . . 2
Dicembre 2025 . . . 2
Controllo dell'accesso alle query con query condivise . . . 2
Filtraggio migliore durante la gestione dei monitor . . . 3
Visualizzazioni della dashboard più pulite . . . 4
Novembre 2025 . . . 4
Imposta la tua home page personalizzata . . . 4
Rimani organizzato con il raggruppamento automatico della dashboard . . . 4
Ottobre 2025 . . . 5
Stato di salute dell'infrastruttura: visibilità immediata sui rischi di storage e fabric . . . 5
Monitor multi-condizione per avvisi precisi . . . 6
Miglioramenti delle query: dettagli degli oggetti a colpo d'occhio . . . 7
Miglioramenti della sicurezza del carico di lavoro . . . 7
Agosto 2025 . . . 8
Dati widget mirati a portata di mano . . . 8
Dashboard di esportazione e importazione . . . 8
Integrazione cloud avanzata: supporto Google Cloud NetApp Volumes (GCNV) . . . 9
Monitoraggio StorageGRID migliorato . . . 9
Supporto del sistema operativo . . . 9
Giugno 2025 . . . 9
VM Analyzer: visibilità olistica da VM a storage e risoluzione dei problemi . . . 9
Supporto del sistema operativo . . . 10
Maggio 2025 . . . 10
Le nuove landing page ti mantengono aggiornato . . . 10
Miglioramenti della sicurezza del carico di lavoro . . . 11
Esportazione asincrona .CSV . . . 13
Aprile 2025 . . . 13
Limiti di anomalia basati su ML nei widget di linea per la risoluzione proattiva dei problemi . . . 13
Ottimizza i costi VMware con il supporto di archiviazione VSAN . . . 14
Dettagli degli avvisi a portata di mano . . . 15
Esportazione asincrona di analisi forense della sicurezza del carico di lavoro . . . 15
Notifiche del Data Collector raggruppate in regole . . . 15
Marzo 2025 . . . 16
Navigazione contestuale migliorata per una gestione efficiente delle infrastrutture . . . 16
Conserva la cronologia delle risorse rimosse . . . 16
Aggiornamento tramite pulsante dell'operatore Kubernetes . . . 17
Test di connettività per i collettori di dati di sicurezza del carico di lavoro di archiviazione . . . 18
Supporto del sistema operativo . . . 18
Febbraio 2025 . . . 19
Monitoraggio dell'utilizzo dell'API DII: migliora la sicurezza e l'efficienza . . . 19

API di sicurezza del carico di lavoro per limitare gli utenti . . . 20
Gennaio 2025 . . . 20
Gestire proattivamente il rischio con Forensics Grouping . . . 20
Controllo degli accessi alla dashboard . . . 21
Dicembre 2024 . . . 22
Presentazione di SAN Analyzer: visibilità migliorata per i carichi di lavoro a blocchi . . . 22
Ottimizza i costi delle VM con la dismissione intelligente degli host e il recupero delle VM . . . 23
Scopri informazioni dettagliate sui registri con il supporto dei grafici temporali e dei widget delle tabelle . . . 24
Novembre 2024 . . . 25
Nuova API per gli avvisi di sicurezza del carico di lavoro . . . 25
Analizza le modifiche di configurazione nel tuo ambiente . . . 25
Supporto KubeVirt: monitora i carichi di lavoro delle macchine virtuali in esecuzione nel tuo cluster Kubernetes . . . 25
Ottobre 2024 . . . 26
Sblocca nuove informazioni con espressioni personalizzate nei monitor . . . 26
Ridurre al minimo le interruzioni degli avvisi durante il periodo di manutenzione . . . 26
Semplifica la gestione degli avvisi con le nuove regole di notifica degli avvisi . . . 27
Analisi dei log nelle dashboard . . . 28
Migliore osservabilità VMware con VMware Events . . . 28
Aggiornamenti del Data Collector: . . . 29
Settembre 2024 . . . 29
Presentazione di Data Infrastructure Insights, precedentemente Cloud Insights . . . 29
Agosto 2024 . . . 29
Visualizza i dati specifici per il tuo intervallo di tempo . . . 29
Analisi del cambiamento e del rapporto di cambiamento (%) . . . 29
Esporta i risultati delle query del registro in .CSV . . . 30
Risolvi gli avvisi in base al tempo . . . 30
Luglio 2024 . . . 31
AIOps: rilevamento delle anomalie . . . 31
Miglioramenti della sicurezza del carico di lavoro . . . 31
Navigazione più semplice nella dashboard . . . 31
Giugno 2024 . . . 32
Supporto del sistema operativo . . . 32
Maggio 2024 . . . 32
Risolvi automaticamente gli avvisi in base al tempo . . . 32
Aprile 2024 . . . 33
Supporto iSCSI per Kubernetes . . . 33
Supporto del sistema operativo . . . 34
Marzo 2024 . . . 34
Dettagli dell'agente di sicurezza del carico di lavoro . . . 34
Rappresenta più dati più rapidamente . . . 34
Febbraio 2024 . . . 35
Miglioramenti dell'usabilità . . . 35
Visualizza tutte le modifiche nel tuo namespace . . . 36

Registri correlati per gli avvisi . . . 37
Raccogliere i dati dello switch ONTAP . . . 37
API del raccoglitore dati per la sicurezza del carico di lavoro . . . 37
Gennaio 2024 . . . 38
Prova le funzionalità di Cloud Insights che non hai ancora utilizzato . . . 38
Quanto sono sani i miei carichi di lavoro? . . . 38
Aggiornamenti del Data Collector . . . 38
Algoritmo ML avanzato per il rilevamento del ransomware . . . 38
Funzionalità deprecate . . . 39
Dicembre 2023 . . . 39
Analisi dei cambiamenti in sintesi . . . 39
Dashboard delle prestazioni del carico di lavoro di Kubernetes . . . 40
Dettagli della query in una schermata . . . 41
Aggiornamenti del Data Collector: . . . 42
Novembre 2023 . . . 42
Sicurezza del carico di lavoro: sospendi/riprendi un collettore . . . 42
Informazioni sul supporto del nodo di archiviazione . . . 43
Mappa i tag VMWare alle annotazioni Cloud Insights . . . 43
Miglioramenti dell'affidabilità del collettore CLI Brocade per FOS 9.1.1c e firmware superiore . . . 43
Ottobre 2023 . . . 43
Sicurezza avanzata del carico di lavoro . . . 43
Prove del modulo . . . 44
Limita l'accesso ai domini specificati . . . 44
Aggiornamenti del Data Collector . . . 44
Settembre 2023 . . . 45
Trova facilmente ciò che desideri nei registri . . . 45
Pannello di dettaglio del registro "fluttuante" . . . 46
Comprimi il menu . . . 47
Miglioramenti del Data Collector . . . 48
Agosto 2023 . . . 48
Raccolta di registri Isilon/PowerScale e dati di analisi avanzata . . . 49
Mappa del carico di lavoro migliorata . . . 49
Regolazione dell'utilizzo delle unità gestite di Kubernetes . . . 49
Modifiche al collezionista/acquisizione: . . . 50
Menu migliorati . . . 50
Luglio 2023 . . . 52
Mostra modifiche recenti . . . 52
Miglioramenti dell'operatore . . . 52
Approfondimento: Recuperare lo stoccaggio a freddo . . . 53
Firma dell'immagine dell'operatore . . . 53
Aggregazione, formattazione condizionale e altro per le query . . . 53
API per l'audit . . . 54
Raccolta dati: Trident Economy . . . 54
Giugno 2023 . . . 54
Controlla il tuo utilizzo . . . 54

Il monitoraggio e la mappa della rete Kubernetes sono disponibili per tutti . . . 55
Modifiche al collezionista/acquisizione: . . . 55
Nuove dashboard ONTAP Essentials . . . 55
Monitor di sistema aggiuntivi . . . 55
Maggio 2023 . . . 56
Installazione migliorata dell'operatore di monitoraggio Kubernetes . . . 56
Virtualizzazione dello storage . . . 56
Nuovi parametri webhook . . . 56
Report sui dati di Kubernetes . . . 56
Monitor di sistema ONTAP predefiniti abilitati per i nuovi clienti . . . 57
Aprile 2023 . . . 57
Monitoraggio e mappa delle prestazioni di Kubernetes . . . 57
Pannello di controllo di sicurezza ONTAP Essentials . . . 58
Reclaim ONTAP Cold Storage . . . 58
La notifica di abbonamento controlla anche i messaggi banner . . . 59
Il reporting ha un nuovo aspetto . . . 59
Monitor in pausa per impostazione predefinita . . . 59
Cerchi la scheda Misurazione API? . . . 59
Marzo 2023 . . . 60
Connessione cloud per ONTAP 9.9+ obsoleta . . . 60
Gennaio 2023 . . . 60
Nuovi monitor di registro . . . 60
Esportazione .CSV per tutti i widget della tabella della dashboard . . . 60
Dicembre 2022 . . . 60
Scopri la protezione dal ransomware e altre funzionalità di sicurezza durante la prova Cloud Insights . . . 60
I carichi di lavoro Kubernetes hanno la loro landing page . . . 60
Controlla i tuoi checksum . . . 61
Miglioramenti degli avvisi di registro . . . 61
11 nuovi monitor ONTAP predefiniti che coprono SnapMirror per la continuità aziendale . . . 62
Novembre 2022 . . . 62
Oltre 40 nuovi monitor di sicurezza, raccolta dati e CVO! . . . 62
Ottobre 2022 . . . 62
Rilevamento ransomware migliore e più accurato con l'integrazione di ONTAP Autonomous Ransomware Protection . . . 62
Settembre 2022 . . . 63
Monitor disponibili in Basic Edition . . . 63
Dashboard ONTAP Power e StorageGRID . . . 63
Visibilità immediata della soglia nelle tabelle . . . 63
Monitor di sicurezza . . . 63
Chatta da qualsiasi luogo . . . 63
Approfondimenti più visibili . . . 64
Nuovi raccoglitori di dati . . . 64
Altri aggiornamenti del Data Collector . . . 64
Supporto del sistema operativo . . . 64
Agosto 2022 . . . 64

- Cloud Insights ha un nuovo look! 64
- Non sai da dove iniziare? Scopri ONTAP Essentials! 65
- Le famiglie di dati di archiviazione vengono unite 66
- Quanta energia consuma il mio storage? 67
- Funzionalità graduate da Anteprima 68
- Come sta andando la mia raccolta dati? 68
- Token API con rinnovo automatico 68
- La Basic Edition ti offre più di prima 69
- Pronti a saperne di più? 69
- Supporto del sistema operativo 69

Giugno 2022 69
- Saturazione del cluster Kubernetes e altri dettagli 69
- Quanti anni ha il tuo cluster Kubernetes? 70
- Previsione del tempo di riempimento della capacità 70
- Cosa è cambiato nel mio ambiente? 71
- Supporto del sistema operativo 71
- Agente Telegraf aggiornato 71
- Funzionalità di anteprima 72

Maggio 2022 72
- Chatta in diretta con il supporto NetApp 72
- Operatore Kubernetes 72
- Gestisci utenti e inviti con API 73
- Avvisi sulla raccolta dati 73
- Avviso sulle modifiche allo storage ONTAP 73
- Funzionalità di anteprima 73

Aprile 2022 74
- Condividi il tuo feedback! 74
- Dashboard Editor aggiornato 74
- Monitoraggio avanzato per la tua infrastruttura Kubernetes 75
- Funzionalità di anteprima 75
- Nuovo raccoglitore di dati 76
- Altri aggiornamenti del Data Collector 76

Marzo 2022 76
- Connessione cloud per ONTAP 9.9+ 76
- Nuovo FSx per i monitor NetApp ONTAP 76
- Nuove funzionalità Cloud Secure disponibili per tutti 77
- Agente Telegraf aggiornato 77
- Aggiornamenti del Data Collector 77

Febbraio 2022 77
- Cloud Insights risolve le vulnerabilità di Apache Log4j 77
- Pagina dei dettagli dello spazio dei nomi Kubernetes 77

Dicembre 2021 78
- Integrazione più profonda per i sistemi ONTAP 78
- Interrogazione dei registri 78
- Notifiche a livello di Data Collector. 79

Maggiore flessibilità dei ruoli Cloud Secure . . . 79
Supporto del sistema operativo . . . 79
Aggiornamenti del Data Collector . . . 79
Novembre 2021 . . . 80
Dashboard adattive . . . 80
Accedi al database di reporting tramite API . . . 81
Tabelle pod nella landing page della VM . . . 81
Aggiornamenti del Data Collector . . . 81
Sistemi operativi aggiuntivi supportati . . . 82
Ottobre 2021 . . . 82
Filtri sulle pagine di K8S Explorer . . . 82
Dati K8s per la segnalazione . . . 82
È arrivato il tema scuro . . . 83
Supporto per la raccolta dati . . . 83
Settembre 2021 . . . 83
Le policy sulle prestazioni ora sono monitor . . . 83
Suggerimenti di completamento automatico, caratteri jolly ed espressioni nei monitor . . . 83
Agente Telegraf aggiornato . . . 84
Supporto per la raccolta dati . . . 84
Agosto 2021 . . . 85
Nuova interfaccia utente della pagina di controllo . . . 85
Gestione avanzata dei ruoli utente . . . 85
Giugno 2021 . . . 85
Suggerimenti di completamento automatico, caratteri jolly ed espressioni nei filtri . . . 85
API disponibili per edizione . . . 86
Visibilità di Kubernetes PV e Pod . . . 86
Collegamenti tra nodi Kubernetes e VM . . . 86
Monitor di avviso che sostituiscono i criteri di prestazione . . . 87
Cloud Secure supporta NFS . . . 88
Eliminazione Cloud Secure . . . 88
Velocità di raccolta dati Cloud Secure . . . 88
Maggio 2021 . . . 88
Agente Telegraf aggiornato . . . 88
Aggiungere azioni correttive a un avviso . . . 89
API di Cloud Insights per tutte le edizioni . . . 89
Aprile 2021 . . . 89
Gestione più semplice dei monitor . . . 89
Opzioni di avviso avanzate tramite webhook . . . 90
Identificazione del dispositivo migliorata . . . 90
Hai chiesto di più! . . . 90
Più abbonamenti in un unico ambiente Cloud Insights . . . 91
Scegli il tuo percorso . . . 91
Onboarding Cloud Secure più semplice . . . 91
Febbraio 2021 . . . 92
Agente Telegraf aggiornato . . . 92

Analizzatore dei costi del cloud . . . 92
Ricerca di oggetti con valori nulli tramite filtri . . . 92
Supporto multi-regione . . . 92
Gennaio 2021 . . . 93
Ulteriori metriche ONTAP rinominate . . . 93
Nuovo Kubernetes Explorer . . . 94
Dicembre 2020 . . . 95
Installazione di Kubernetes più semplice . . . 95
Novembre 2020 . . . 95
Dashboard aggiuntive . . . 95
Rinomina colonna nei widget tabella . . . 96
Ottobre 2020 . . . 96
Espansione predefinita dei dati di integrazione . . . 96
Supporto tecnico dell'edizione base . . . 96
API pubblica Cloud Secure . . . 97
Settembre 2020 . . . 97
Pagina di query con dati di integrazione . . . 97
Formattazione della visualizzazione dell'unità nel widget Tabella . . . 97
Pagina dei dettagli dell'unità di acquisizione . . . 98
Dipendenza Docker Cloud Secure rimossa . . . 98
Segnalazione dei ruoli utente . . . 98
Nuova categoria API per l'inserimento dei dati . . . 99
Agosto 2020 . . . 99
Monitoraggio e allerta . . . 99
Luglio 2020 . . . 99
Cloud Secure *Esegui un'istantanea* Azione . . . 100
Aggiornamenti metrici/contatori . . . 101
Rilevamento di potenziali attacchi Cloud Secure . . . 101
Iscriviti alla Premium Edition tramite AWS . . . 102
Widget tabella migliorato . . . 102
Filtraggio delle metriche . . . 104
Dati contatore avanzati ONTAP . . . 104
Dashboard dei contatori avanzati . . . 106
Saperne di più . . . 106
Menu Norme e violazioni . . . 106
Agente Telegraf aggiornato . . . 106
Giugno 2020 . . . 107
Segnalazione errori semplificata del Data Collector . . . 107
Miglioramenti dei widget . . . 107
Maggio 2020 . . . 108
Segnalazione dei ruoli utente . . . 108
Aggiornamenti Cloud Secure . . . 109
Raggruppamento della dashboard . . . 109
Fissaggio della dashboard . . . 110
Modalità TV e aggiornamento automatico . . . 110

Aprile 2020 . . . 111
Nuove scelte di intervallo di tempo della dashboard . . . 111
Aggiornamenti Cloud Secure . . . 111
Ora predefinita della dashboard . . . 111
Tempi di aggregazione ottimizzati . . . 111
Formato automatico dell'unità di visualizzazione . . . 111
Importa annotazioni tramite API . . . 112
Selettore widget più semplice . . . 112
Febbraio 2020 . . . 113
API con edizione Premium . . . 113
Polling iniziale dopo l'aggiunta di un raccoglitore dati . . . 113
Duplicazione dei widget più semplice . . . 114
Accesso singolo (SSO) . . . 114
Gennaio 2020 . . . 114
Documentazione Swagger per REST API . . . 115
Barra di avanzamento dei tutorial sulle funzionalità . . . 115
Modifiche all'unità di acquisizione . . . 115
Aggregazione temporale ottimizzata nei widget . . . 115
Procedura semplificata "Introduzione a Cloud Insights" . . . 115
Onboarding Data Infrastructure Insights . . . 117
Sicurezza . . . 118
Data Infrastructure Insights . . . 118
Panoramica sulla sicurezza . . . 118
Informazioni e Regione . . . 120
Quali informazioni memorizza Data Infrastructure Insights ? . . . 120
Dove vengono archiviate le mie informazioni? . . . 121
Ulteriori informazioni . . . 122
Strumento SecurityAdmin . . . 122
Considerazioni sull'aggiornamento e l'installazione . . . 122
Gestione della sicurezza sull'unità di acquisizione . . . 123
Prima di iniziare . . . 123
Utilizzo dello strumento SecurityAdmin . . . 123
Specificare un utente per eseguire lo strumento . . . 125
Aggiornamento o rimozione del proxy . . . 126
Recupero della chiave esterna . . . 128
Crittografia di una password per l'uso nell'API . . . 128
Iniziare . . . 132
Introduzione ai tutorial video . . . 132
Lista di controllo e tutorial video . . . 132
Video tutorial . . . 133
Raccolta dati . . . 133
Come iniziare a raccogliere dati . . . 133
Requisiti dell'unità di acquisizione . . . 136
Configurazione delle unità di acquisizione . . . 138
Configurazione di un agente per la raccolta di dati (Windows/Linux) . . . 145

Configurazione dei raccoglitori di dati . . . 156
Determinazione dello stato di acquisizione del raccoglitore dati . . . 157
Gestione dei raccoglitori di dati configurati . . . 157
Ricerca di un raccoglitore di dati fallito . . . 159
Importazione di dashboard . . . 160
Importazione dalla Galleria della Dashboard . . . 160
Importazione di una dashboard esportata . . . 160
Account utente e ruoli . . . 161
Livelli di autorizzazione . . . 161
Creazione di account invitando utenti . . . 164
Modifica del ruolo di un utente esistente . . . 166
Eliminazione degli utenti . . . 167
Single Sign-On (SSO) e federazione delle identità . . . 167
Limitazione dell'accesso per dominio . . . 169
Elenco di riferimento del Data Collector di Data Infrastructure Insights . . . 171
Iscrizione a Data Infrastructure Insights . . . 175
Edizione di prova . . . 175
Prova tramite AWS Marketplace . . . 176
Cosa succede se il mio periodo di prova è scaduto? . . . 176
Cosa succede se il mio **abbonamento** è scaduto? . . . 176
Valutazione del modulo . . . 176
Estimatore . . . 177
Opzioni di abbonamento . . . 178
Misurazione dell'osservabilità . . . 178
Misurazione della sicurezza del carico di lavoro . . . 179
Come posso abbonarmi? . . . 179
Iscriviti tramite NetApp Sales Direct . . . 179
Auto-iscrizione tramite AWS Marketplace . . . 179
Visualizza lo stato del tuo abbonamento . . . 180
Visualizza la tua gestione dell'utilizzo . . . 181
Cosa succede se supero l'utilizzo a cui sono iscritto? . . . 181
Iscriviti direttamente e salta la prova . . . 182
Aggiunta di un ID di autorizzazione . . . 182
Osservabilità . . . 183
Creazione di dashboard . . . 183
Panoramica delle dashboard . . . 183
Funzionalità della dashboard . . . 187
Gestione degli accessi alla dashboard . . . 220
Best Practice per Dashboard e Widget . . . 222
Dashboard di esempio . . . 225
Lavorare con le query . . . 230
Interrogazione di asset e metriche . . . 230
Creazione di query . . . 231
Visualizzazione delle query . . . 238
Esportazione dei risultati della query in un file .CSV . . . 238

Modifica o eliminazione di una query . . . 239
Assegnazione di più applicazioni o rimozione di più applicazioni dalle risorse . . . 240
Copia dei valori della tabella . . . 241
Esploratore di log . . . 241
Identificazione dei dispositivi inattivi . . . 247
Approfondimenti . . . 248
Approfondimenti . . . 248
Approfondimenti: risorse condivise sotto stress . . . 248
Approfondimenti: gli spazi dei nomi di Kubernetes stanno esaurendo lo spazio . . . 251
Approfondimenti: Reclaim ONTAP Cold Storage . . . 252
Monitor e avvisi . . . 255
Avvisi con monitor . . . 255
Visualizzazione e gestione degli avvisi dai monitor . . . 266
Configurazione delle notifiche e-mail . . . 269
Monitor di rilevamento delle anomalie . . . 272
Monitor di sistema . . . 276
Notifiche webhook . . . 355
Lavorare con le annotazioni . . . 369
Definizione delle annotazioni . . . 369
Utilizzo delle annotazioni . . . 372
Creazione di regole di annotazione . . . 374
Importazione di annotazioni . . . 376
Lavorare con le applicazioni . . . 378
Monitoraggio dell'utilizzo delle risorse per applicazione . . . 378
Creazione di applicazioni . . . 379
Risoluzione automatica del dispositivo . . . 380
Panoramica sulla risoluzione automatica del dispositivo . . . 380
Regole di risoluzione del dispositivo . . . 383
Risoluzione del dispositivo Fibre Channel . . . 385
Risoluzione del dispositivo IP . . . 388
Impostazione delle opzioni nella scheda Preferenze . . . 390
Esempi di espressioni regolari . . . 391
Informazioni sulla pagina delle risorse . . . 397
Panoramica della pagina delle risorse . . . 397
Filtraggio per oggetti nel contesto . . . 403
Virtualizzazione dello storage . . . 404
Suggerimenti e consigli per cercare risorse e avvisi . . . 406
Analisi dei dati . . . 408
Panoramica dell'analizzatore SAN . . . 408
Panoramica di VM Analyzer . . . 411
Monitorare lo stato di salute delle infrastrutture . . . 413
Segnalazione . . . 414
Panoramica dei report di Data Infrastructure Insights Insights . . . 415
Ruoli utente dei report di Data Infrastructure Insights . . . 416
Report predefiniti semplificati . . . 418

Dashboard del gestore dell'archiviazione . . . 421
Creazione di un report (esempio) . . . 424
Gestione dei report . . . 427
Creazione di report personalizzati . . . 430
Accedi al database di reporting tramite API . . . 438
Pubblicazione e annullamento della pubblicazione di annotazioni per la segnalazione . . . 442
Come vengono conservati i dati storici per la creazione di report . . . 443
Diagrammi di schema di reporting Data Infrastructure Insights . . . 444
Schemi Data Infrastructure Insights per la creazione di report . . . 496
Kubernetes . . . 498
Panoramica del cluster Kubernetes . . . 498
Perfezionamento del filtro . . . 498
Prima di installare o aggiornare NetApp Kubernetes Monitoring Operator . . . 499
Cose importanti da notare prima di iniziare . . . 500
Installazione e configurazione dell'operatore di monitoraggio Kubernetes . . . 503
Prima di installare Kubernetes Monitoring Operator . . . 503
Installazione dell'operatore di monitoraggio Kubernetes . . . 504
Componenti di monitoraggio di Kubernetes . . . 506
Aggiornamento all'ultima versione di Kubernetes Monitoring Operator . . . 506
Arresto e avvio dell'operatore di monitoraggio Kubernetes . . . 508
Disinstallazione . . . 508
Informazioni su Kube-state-metrics . . . 509
Configurazione/Personalizzazione dell'operatore . . . 509
Una nota sui segreti . . . 513
Verifica delle firme delle immagini degli operatori di monitoraggio di Kubernetes . . . 514
Risoluzione dei problemi . . . 515
Opzioni di configurazione dell'operatore di monitoraggio Kubernetes . . . 524
File di configurazione dell'agente di esempio . . . 524
Pagina dei dettagli del cluster Kubernetes . . . 542
Conteggio di spazi dei nomi, nodi e pod . . . 542
Risorse condivise e saturazione . . . 542
Spazi dei nomi . . . 542
Carichi di lavoro . . . 543
La "Ruota" del Cluster . . . 543
Una nota sugli indicatori . . . 546
Monitoraggio e mappa delle prestazioni della rete Kubernetes . . . 546
Prerequisiti . . . 547
Monitor . . . 548
La mappa . . . 548
Dettagli e avvisi sul carico di lavoro . . . 550
Ricerca e filtraggio . . . 550
Etichette del carico di lavoro . . . 551
Immergiti in profondità . . . 552
Analisi delle modifiche di Kubernetes . . . 554
Filtraggio . . . 555

Stato rapido . . . 556
Pannello di dettaglio . . . 557
Elementi essenziali ONTAP . . . 559
Panoramica . . . 559
Protezione dei dati . . . 560
Sicurezza . . . 561
Avvisi . . . 564
Infrastruttura . . . 565
Networking . . . 566
Carichi di lavoro . . . 566
Amministrazione e altre attività . . . 568
API Data Infrastructure Insights . . . 568
Requisiti per l'accesso all'API . . . 568
Documentazione API (Swagger) . . . 568
Token di accesso API . . . 569
Tipo di API . . . 570
Attraversamento dell'inventario . . . 570
Si espande . . . 571
Dati sulle prestazioni . . . 573
Metriche delle prestazioni degli oggetti . . . 575
Dati storici delle prestazioni . . . 575
Oggetti con attributi di capacità . . . 576
Utilizzo della ricerca per cercare oggetti . . . 577
Disabilitazione o revoca di un token API . . . 577
Rotazione dei token di accesso API scaduti . . . 578
Monitoraggio dell'ambiente . . . 579
Revisione contabile . . . 579
Digital Advisor Active IQ . . . 582
Sicurezza del carico di lavoro . . . 585
Informazioni sulla sicurezza del carico di lavoro di archiviazione . . . 585
Visibilità . . . 585
Protezione . . . 585
Conformità . . . 585
Iniziare . . . 585
Introduzione alla sicurezza del carico di lavoro . . . 585
Requisiti dell'agente di sicurezza del carico di lavoro . . . 586
Distribuisci agenti di sicurezza del carico di lavoro . . . 590
Eliminazione di un agente di sicurezza del carico di lavoro . . . 597
Configurazione di un raccoglitore di directory utente di Active Directory (AD) . . . 598
Configurazione di un server di raccolta directory LDAP . . . 603
Configurazione del raccoglitore dati ONTAP SVM . . . 608
Risoluzione dei problemi del raccoglitore dati ONTAP SVM . . . 619
Configurazione di Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP . . . 625
Gestione degli utenti . . . 627
Event Rate Checker: Guida alle dimensioni degli agenti . . . 628

Comprendere e indagare gli avvisi . . . 631
Attenzione . . . 632
Opzioni filtro . . . 633
La pagina Dettagli avviso . . . 633
Scatta un'istantanea Azione . . . 635
Notifiche di avviso . . . 636
Politica di conservazione . . . 636
Risoluzione dei problemi . . . 637
Medicina legale . . . 637
Analisi forense - Tutte le attività . . . 638
Panoramica utente forense . . . 648
Criteri di risposta automatizzati . . . 649
Criteri sui tipi di file consentiti . . . 651
Integrazione con la protezione autonoma dai ransomware ONTAP . . . 652
Prerequisiti . . . 653
Autorizzazioni utente richieste . . . 653
Esempio di avviso . . . 653
Limitazioni . . . 654
Risoluzione dei problemi . . . 654
Integrazione con ONTAP Accesso negato . . . 655
Prerequisiti . . . 655
Autorizzazioni utente richieste . . . 656
Eventi di accesso negato . . . 656
Blocco dell'accesso degli utenti per fermare gli attacchi . . . 657
Prerequisiti per il blocco dell'accesso utente . . . 657
Come abilitare la funzionalità? . . . 658
Come impostare il blocco automatico dell'accesso degli utenti? . . . 658
Come sapere se ci sono utenti bloccati nel sistema? . . . 658
Limitare e gestire manualmente l'accesso degli utenti . . . 658
Cronologia delle limitazioni di accesso utente . . . 658
Come disattivare la funzione? . . . 659
Ripristina manualmente gli IP per NFS . . . 659
Ripristina manualmente gli utenti per SMB . . . 660
Risoluzione dei problemi . . . 661
Sicurezza del carico di lavoro: simulazione della manomissione dei file . . . 662
Cose da notare prima di iniziare . . . 663
Linee guida: . . . 663
Passaggi: . . . 663
Generare i file di esempio a livello di programmazione: . . . 664
Riprendi il collezionista . . . 665
Generare i file di esempio a livello di programmazione: . . . 665
Genera un avviso in Workload Security . . . 666
Attivazione dell'avviso più volte . . . 667
Configurazione delle notifiche e-mail per avvisi, avvertenze e stato di integrità dell'agente/collettore dell'origine dati . . . 667

Avvisi e avvisi di potenziali attacchi . . . 667
Monitoraggio dello stato di salute dell'agente e del raccoglitore dati . . . 667
Ricezione di notifiche di aggiornamento dell'agente e del raccoglitore dati . . . 668
Risoluzione dei problemi . . . 668
Notifiche webhook . . . 668
Notifiche di sicurezza del carico di lavoro tramite webhook . . . 668
Esempio di webhook di sicurezza del carico di lavoro per Discord . . . 674
Esempio di webhook di sicurezza del carico di lavoro per PagerDuty . . . 677
Esempio di webhook di sicurezza del carico di lavoro per Slack . . . 681
Esempio di webhook di sicurezza del carico di lavoro per Microsoft Teams . . . 686
API di sicurezza del carico di lavoro . . . 691
Documentazione API (Swagger) . . . 691
Token di accesso API . . . 691
Script per estrarre dati tramite API . . . 692
Risoluzione dei problemi del raccoglitore dati ONTAP SVM . . . 692
Risoluzione dei problemi . . . 700
Risoluzione dei problemi generali Data Infrastructure Insights . . . 700
Problemi di accesso . . . 700
Altri problemi . . . 701
Risorse . . . 701
Risoluzione dei problemi dell'unità di acquisizione su Linux . . . 702
Considerazioni su proxy e firewall . . . 704
Risorse . . . 705
Risoluzione dei problemi dell'unità di acquisizione su Windows . . . 705
Considerazioni su proxy e firewall . . . 707
Risorse . . . 708
Ricerca di un raccoglitore di dati fallito . . . 708
Matrice di supporto del collettore dati Data Infrastructure Insights . . . 709
Archiviazione HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ . . . 709
Amazon AWS EC2 . . . 727
Amazon AWS S3 . . . 733
Azure NetApp Files . . . 737
Switch Fibre Channel Brocade . . . 746
Consulente di rete Brocade HTTP . . . 757
Brocade FOS REST . . . 761
Switch Cisco MDS e Nexus Fabric . . . 771
Coesità . . . 779
EMC Celerra (SSH) . . . 786
EMC CLARiiON (NaviCLI) . . . 795
Dominio dati EMC (SSH) . . . 811
EMC ECS . . . 820
Dell EMC Isilon e PowerScale Rest . . . 828
Dell EMC Isilon / PowerScale (CLI) . . . 847
EMC PowerStore REST . . . 862
EMC RecoverPoint (HTTP) . . . 878

EMC ScaleIO e PowerFlex REST . . . 881
Interfaccia a riga di comando EMC Symmetrix . . . 886
Dell Unisphere REST . . . 905
EMC VNX (SSH) . . . 922
EMC VNXe e Unity Unisphere (CLI) . . . 941
EMC VPLEX . . . 954
EMC XtremIO (HTTP) . . . 963
NetApp E-Series . . . 977
Pure Storage FlashBlade REST . . . 990
Google Cloud Compute . . . 1000
Google Cloud Netapp Volumi . . . 1005
HDS HCP (HTTPS) . . . 1015
Gestione dispositivi HiCommand . . . 1020
Centro operativo Hitachi . . . 1034
HDS HNAS (CLI) . . . 1049
Storage HPE Nimble/Alletra 6000 . . . 1059
Huawei OceanStor (REST/HTTPS) . . . 1072
IBM Cleversafe . . . 1091
IBM DS 8K (DSCLI) . . . 1096
IBM PowerVM (SSH) . . . 1107
IBM SVC (CLI) . . . 1110
IBM XIV e A9000 (XIVCLI) . . . 1125
Infinidat Infinibox (HTTP) . . . 1131
Microsoft Azure Compute . . . 1140
Microsoft Hyper-V . . . 1146
Modalità NetApp 7 . . . 1156
NetApp E-Series REST . . . 1180
Amazon FSx for NetApp ONTAP . . . 1189
NetApp Clustered Data ONTAP 8.1.1+ . . . 1212
ASA . . . 1252
NetApp ONTAP REST . . . 1265
NetApp SolidFire 8.1+ . . . 1287
NetApp StorageGRID (HTTPS) . . . 1304
Archiviazione Nutanix (REST) . . . 1314
OpenStack (API REST / SSH) . . . 1327
Oracle ZFS (HTTPS) . . . 1331
Pure Storage FlashArray (HTTP) . . . 1346
Red Hat RHV (REST) . . . 1358
Rubrik Storage . . . 1363
VAST DataStore . . . 1374
Centro virtuale NetApp HCI . . . 1385
VMware Cloud su AWS . . . 1396
VMware vSphere (servizi Web) . . . 1402
Riferimenti e supporto . . . 1416
Richiesta di supporto . . . 1416

Attivazione del diritto al supporto . . . 1416
Ottenere informazioni di supporto . . . 1419
Matrice di supporto del collettore dati Data Infrastructure Insights . . . 1420
Riferimento al Data Collector - Infrastruttura . . . 1420
Riferimento specifico del fornitore . . . 1420
Configurazione del raccoglitore dati Amazon EC2 . . . 1421
Raccoglitore dati Amazon FSx for NetApp ONTAP . . . 1424
Configurazione del raccoglitore dati di calcolo di Azure . . . 1426
Broadcom . . . 1428
Raccoglitore dati Cisco MDS Fabric Switch . . . 1435
Raccoglitore dati Cohesity SmartFiles . . . 1438
Dell . . . 1439
Dell EMC . . . 1440
Raccoglitore dati Fujitsu Eternus . . . 1465
Raccoglitore dati NetApp Google Compute . . . 1466
Raccoglitore dati Google Cloud NetApp Volumes . . . 1468
HP Enterprise . . . 1469
Sistemi di dati Hitachi . . . 1477
Raccoglitore dati Infinidat InfiniBox . . . 1485
Raccoglitore dati Huawei OceanStor . . . 1486
IBM . . . 1488
Raccoglitore dati Lenovo . . . 1495
Microsoft . . . 1496
NetApp . . . 1499
Raccoglitore dati Nutanix NX . . . 1539
Raccoglitore dati Oracle ZFS Storage Appliance . . . 1540
Raccoglitore dati Pure Storage FlashArray . . . 1542
Raccoglitore dati di Red Hat Virtualization . . . 1544
Raccoglitore dati CDM Rubrik . . . 1545
Configurazione del raccoglitore dati VMware VSphere . . . 1546
Riferimento al Data Collector - Servizi . . . 1549
Raccolta dati nodo . . . 1549
Raccoglitore dati ActiveMQ . . . 1552
Apache Data Collector . . . 1554
Consul Data Collector . . . 1557
Couchbase Data Collector . . . 1558
CouchDB Data Collector . . . 1560
Docker Data Collector . . . 1562
Raccoglitore dati Elasticsearch . . . 1569
Flink Data Collector . . . 1571
Raccoglitore dati Hadoop . . . 1578
Raccoglitore dati HAProxy . . . 1583
Raccoglitore dati JVM . . . 1589
Raccoglitore di dati Kafka . . . 1594
Kibana Data Collector . . . 1597

Installazione e configurazione dell’operatore di monitoraggio Kubernetes . . . 1599
Memcached Data Collector . . . 1619
Raccoglitore dati MongoDB . . . 1622
Raccoglitore dati MySQL . . . 1624
Raccoglitore dati Netstat . . . 1629
Raccoglitore dati Nginx . . . 1630
Raccoglitore dati PostgreSQL . . . 1633
Raccoglitore di dati dell’agente fantoccio . . . 1635
Redis Data Collector . . . 1637
Riferimento alle icone degli oggetti . . . 1639
Icone dell’infrastruttura: . . . 1639
Icone di Kubernetes: . . . 1639
Icone di monitoraggio delle prestazioni di rete e mappa di Kubernetes: . . . 1640
Note legali . . . 1641
Copyright . . . 1641
Marchi . . . 1641
Brevetti . . . 1641
Politica sulla riservatezza . . . 1641
Open source . . . 1641

Documentazione Data Infrastructure Insights

NetApp Data Infrastructure Insights (in precedenza Cloud Insights) è uno strumento di monitoraggio dell'infrastruttura cloud che offre visibilità sull'intera infrastruttura. Con Data Infrastructure Insights puoi monitorare, risolvere i problemi e ottimizzare tutte le tue risorse, inclusi i tuoi cloud pubblici e i tuoi data center privati.

Cosa può fare per me Data Infrastructure Insights ?

Data Infrastructure Insights fornisce un monitoraggio multicloud ibrido, garantendo l'osservabilità completa dell'infrastruttura e dei carichi di lavoro.

- Raccoglitori di dati per infrastrutture e carichi di lavoro eterogenei, incluso Kubernetes
- Collettore Telegraf aperto e API aperte per una facile integrazione
- Avvisi e notifiche completi
- Apprendimento automatico per informazioni intelligenti
- Ottimizzare l'utilizzo delle risorse
- Dashboard integrate o personalizzabili con filtri avanzati per ridurre al minimo il rumore di visualizzazione per rispondere alle domande
- Scopri lo stato di salute delle tue operazioni di archiviazione ONTAP
- Proteggi la tua risorsa aziendale più preziosa – i dati – da manomissioni di file o attacchi di distruzione di dati

---

Iniziare

- Come faccio a**iniziamo** con Data Infrastructure Insights?
- Sono iscritto. Adesso cosa faccio?"Acquisizione dei dati" "Impostazione degli utenti"
- Eccezionale! Cosa succederà adesso?"Preparazione delle risorse: annotazione" "Trovare le risorse desiderate: query" "Visualizzare i dati desiderati: dashboard" "Monitoraggio e avvisi" "Protezione dei dati"
- Questa è roba fantastica! Sono pronto a**iscriviti** .

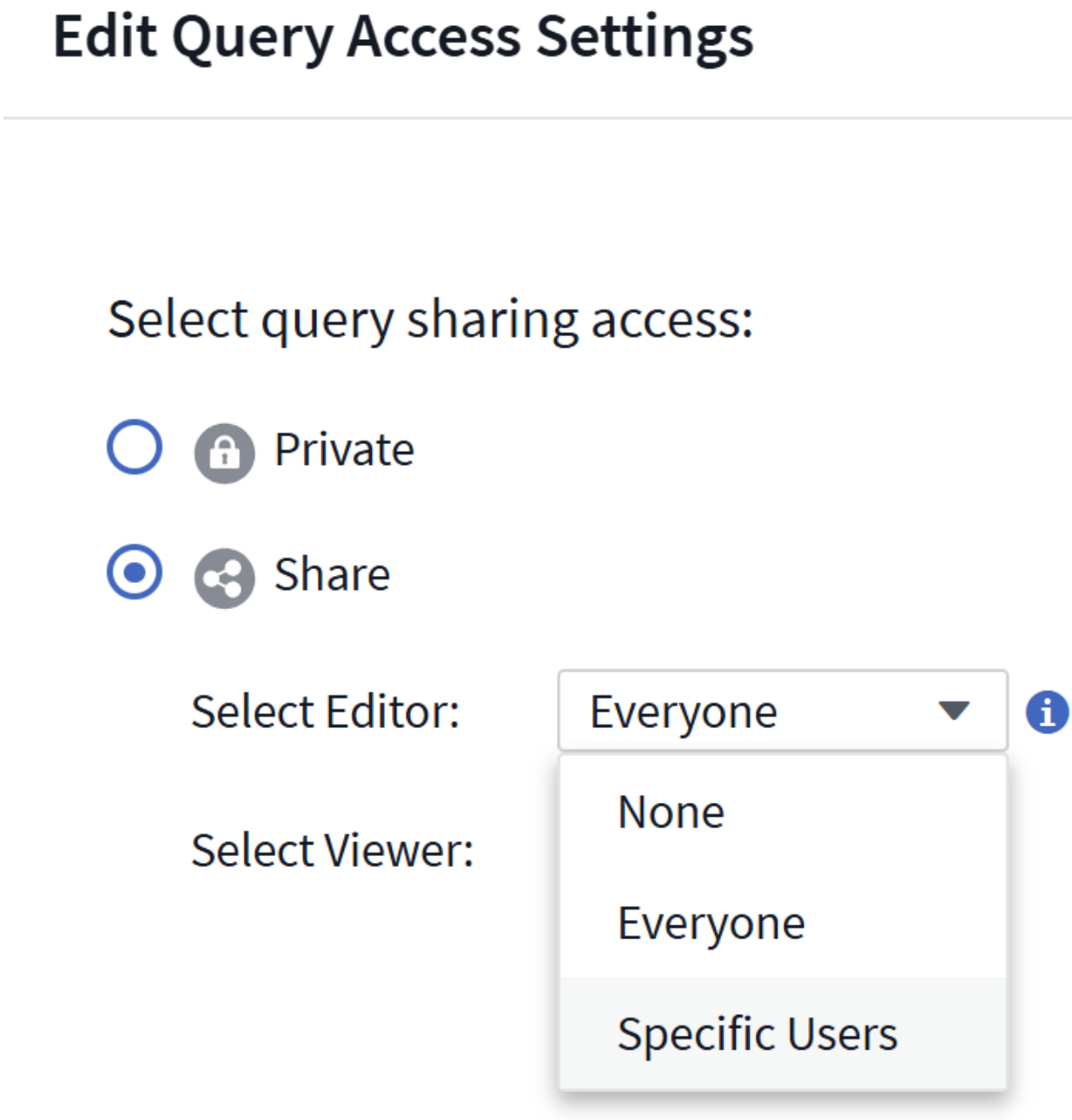
Novità di Data Infrastructure Insights

NetApp migliora e potenzia costantemente i suoi prodotti e servizi. Ecco alcune delle ultime funzionalità e caratteristiche disponibili in Data Infrastructure Insights (in precedenza Cloud Insights).

Dicembre 2025

Controllo dell'accesso alle query con query condivise

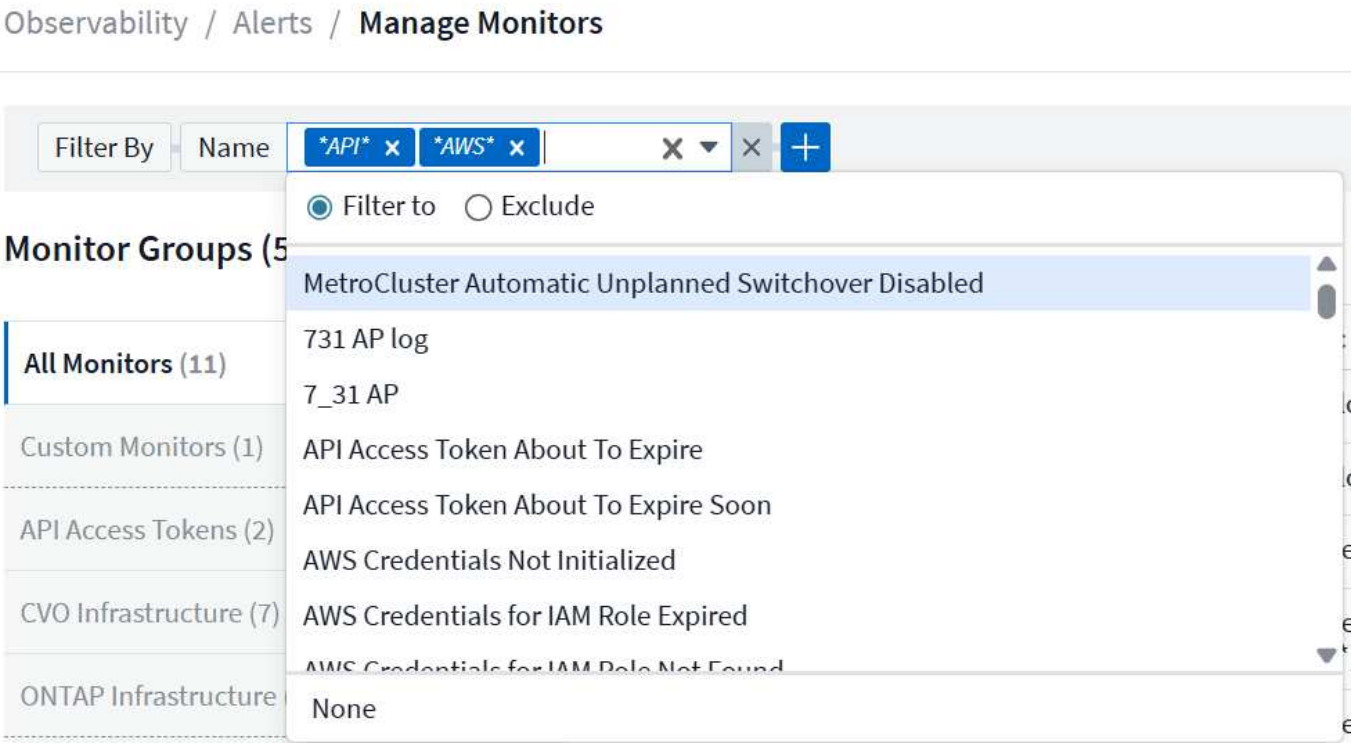
Condividi le query che crei con controlli di autorizzazione dettagliati. Selezionare la modalità Visualizzatore di sola lettura per impedire modifiche o la modalità Modifica per consentirle. Le query private sono accessibili ai creatori, mentre le query condivise possono essere sfruttate nelle regole di annotazione o duplicate per casi d'uso specializzati, offrendoti il controllo completo su come le query vengono utilizzate e modificate all'interno della tua organizzazione.



Inoltre, gli utenti con ruolo *Ospite* possono ora creare e gestire le proprie query private.

Filtraggio migliore durante la gestione dei monitor

Il filtraggio per gli elenchi e i gruppi di Monitor è stato migliorato per aggiungere il supporto dei caratteri jolly, filtri multipli, funzionalità di inclusione/esclusione e altro ancora.



Visualizzazioni della dashboard più pulite

Il design migliorato della dashboard ti aiuta a vedere ciò che conta di più. Maggiore chiarezza visiva con bordi ombreggiati che separano i widget e linee di separazione rimosse per ridurre l'ingombro e consentirti di concentrarti sulle informazioni sui dati. Questi perfezionamenti creano un'esperienza di dashboard più pulita e intuitiva, che consente di individuare tendenze e anomalie in modo più rapido e semplice.

Novembre 2025

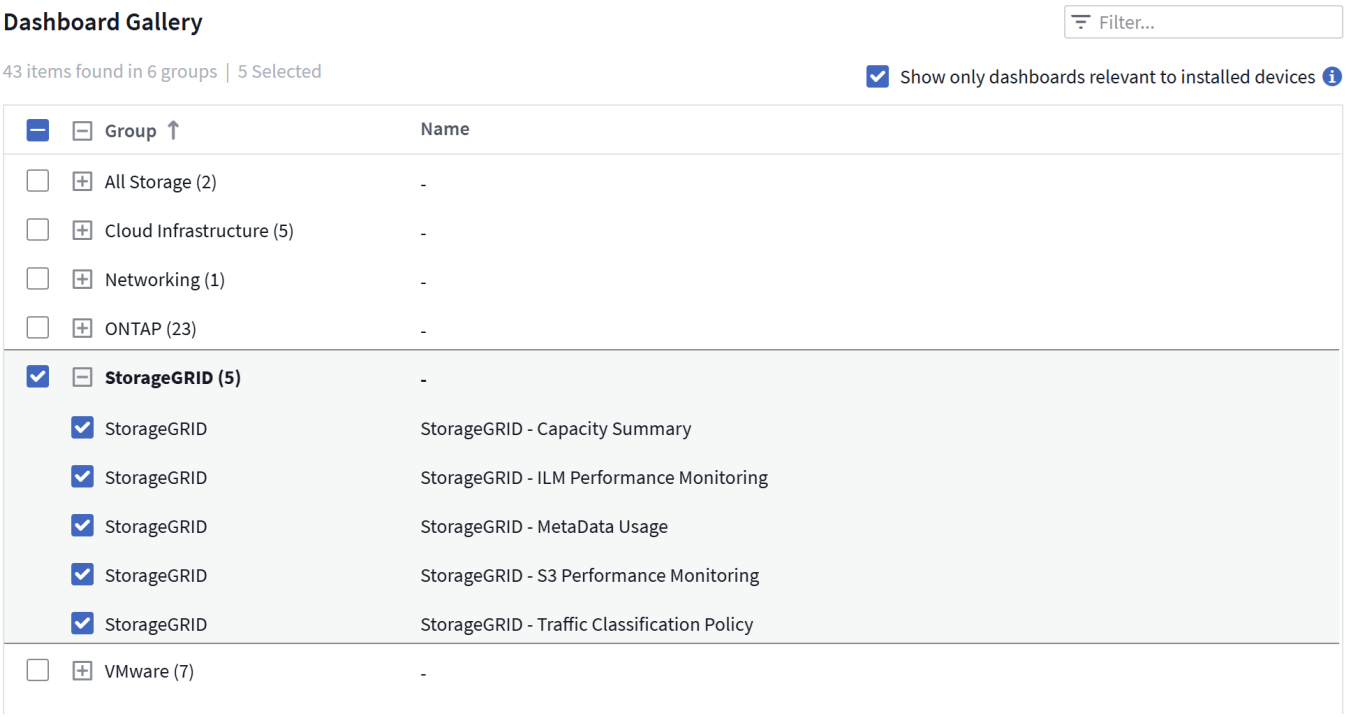
Imposta la tua home page personalizzata

Semplifica il tuo flusso di lavoro di monitoraggio giornaliero impostando *qualsiasi* pagina Data Infrastructure Insights come home page personalizzata. Ogni utente può selezionare una home page diversa per concentrarsi su ciò che è importante per lui: una dashboard critica, avvisi, stato dell'infrastruttura, sicurezza del carico di lavoro o altro ancora.

Rimani organizzato con il raggruppamento automatico della dashboard

Trasforma la tua esperienza con la dashboard con un raggruppamento intelligente che organizza automaticamente le dashboard della Galleria importate in categorie logiche. La nuova funzionalità di

raggruppamento semplifica l'importazione dei dashboard e posiziona ciascun dashboard nel gruppo appropriato in base alla sua funzione e alla sua pertinenza per l'ambiente.

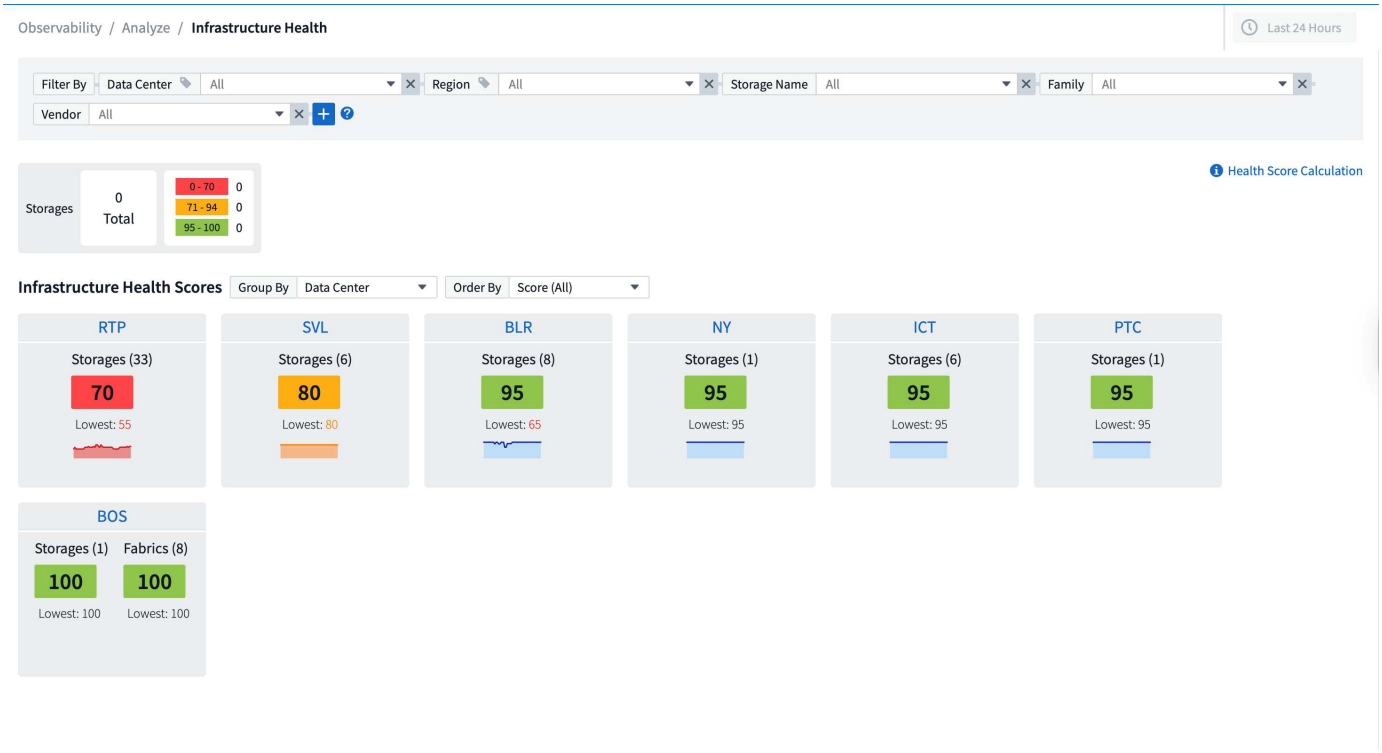


Ottobre 2025

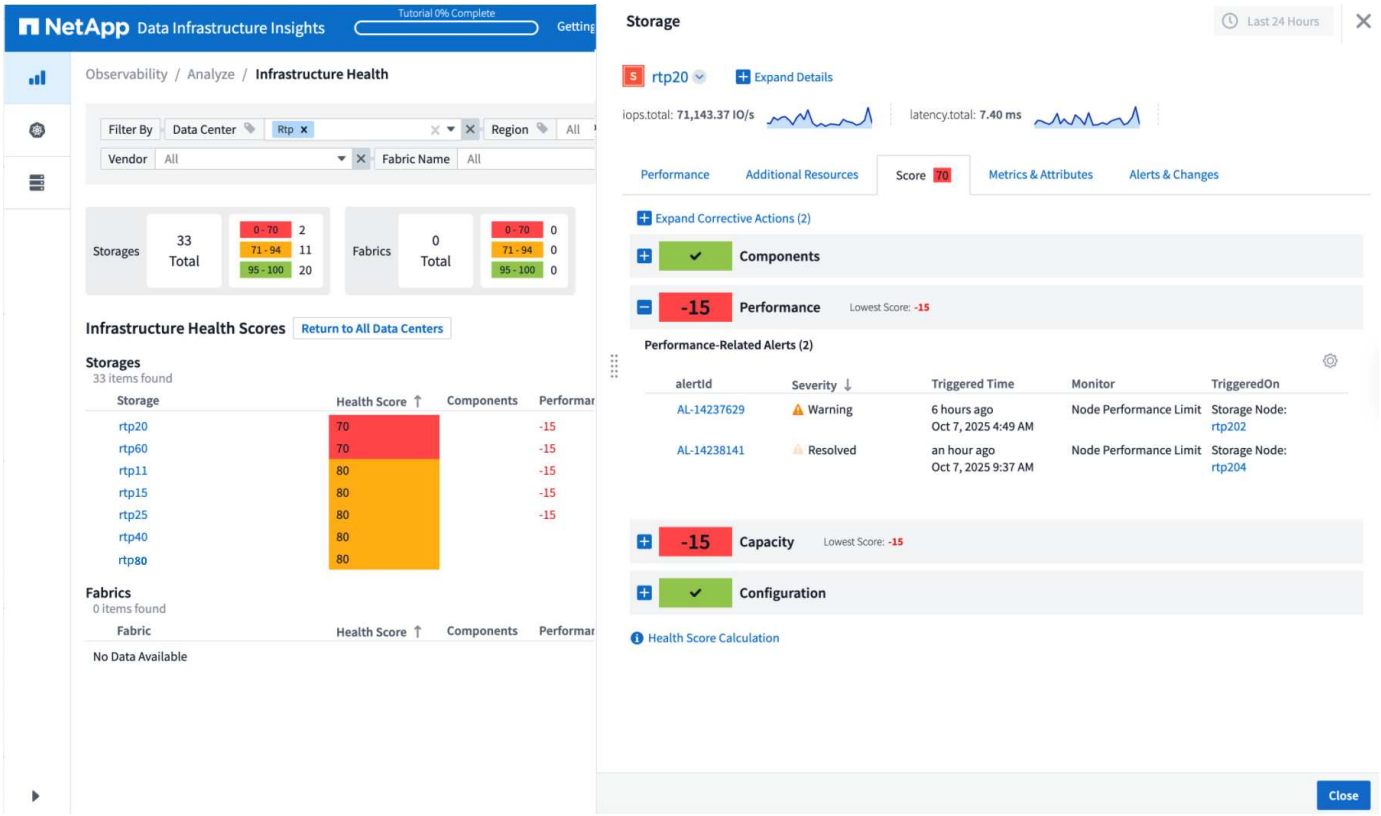
Stato di salute dell'infrastruttura: visibilità immediata sui rischi di storage e fabric

Ottieni visibilità immediata sui potenziali rischi per il tuo storage e i tuoi fabric con la nostra nuova funzionalità **Infrastructure Health**. Un'unica dashboard con codice colore ti offre una visibilità unificata dei rischi, aiutandoti a ridurre al minimo i tempi di inattività e ad alleviare rapidamente le perdite di fatturato.

I punteggi inferiori a 100 indicano potenziali problemi; più basso è il punteggio, meno sane sono le risorse. Raggruppando le risorse per data center o regione per ottenere punteggi di integrità intuitivi e consolidati, è possibile stabilire facilmente le priorità e risolvere i problemi delle aree critiche.



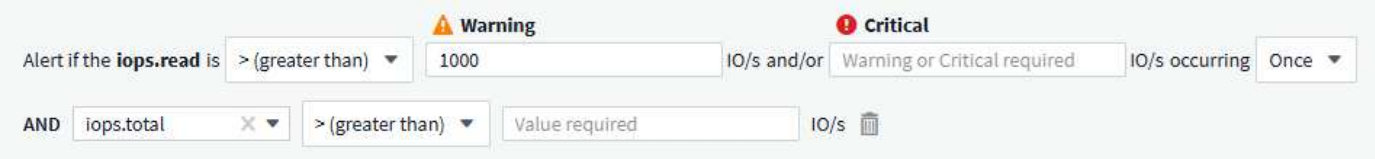
Con un semplice clic, puoi visualizzare informazioni dettagliate in un pannello scorrevole sullo schermo, individuando rapidamente i problemi che richiedono attenzione e mantenendo i tuoi sistemi sicuri e resilienti.



Monitor multi-condizione per avvisi precisi

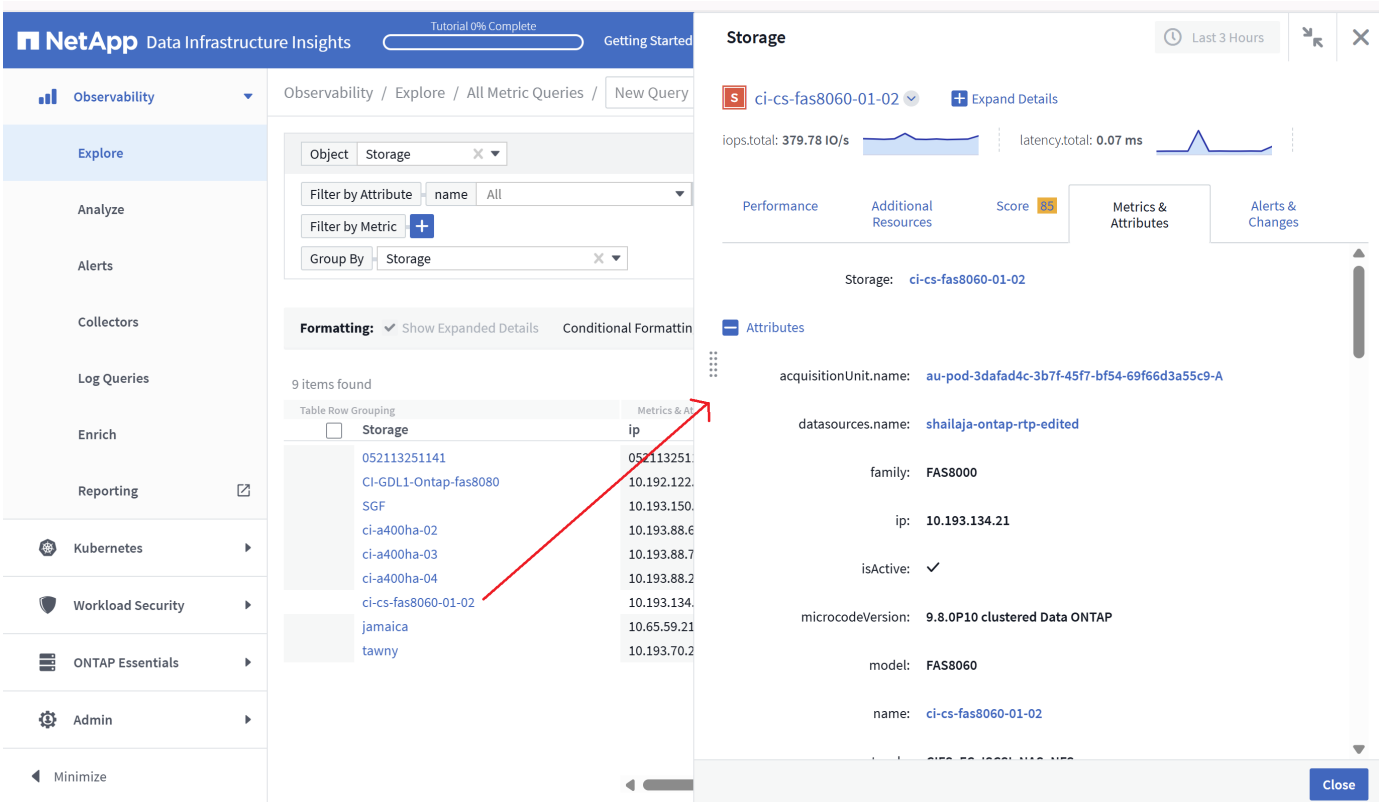
Riduci il rumore degli avvisi e migliora la precisione del monitoraggio aggiungendo una seconda condizione facoltativa a qualsiasi monitor metrico. Gli avvisi vengono attivati solo quando entrambe le condizioni sono

soddisfatte, fornendoti notifiche più mirate che si concentrano sugli scenari che più ti interessano.



Miglioramenti delle query: dettagli degli oggetti a colpo d'occhio

Selezionando una riga nell'elenco dei risultati di una query di un oggetto si apre un pannello dei dettagli per l'oggetto selezionato. Visualizza rapidamente metriche e attributi (la visualizzazione predefinita per le query sugli oggetti), avvisi e modifiche, punteggi di prestazioni e integrità oppure esplora risorse correlate. Tutte le informazioni rilevanti sull'oggetto sono a portata di mano.



Miglioramenti della sicurezza del carico di lavoro

Due nuove API ti offrono un maggiore controllo sul tuo ambiente di sicurezza dei carichi di lavoro:

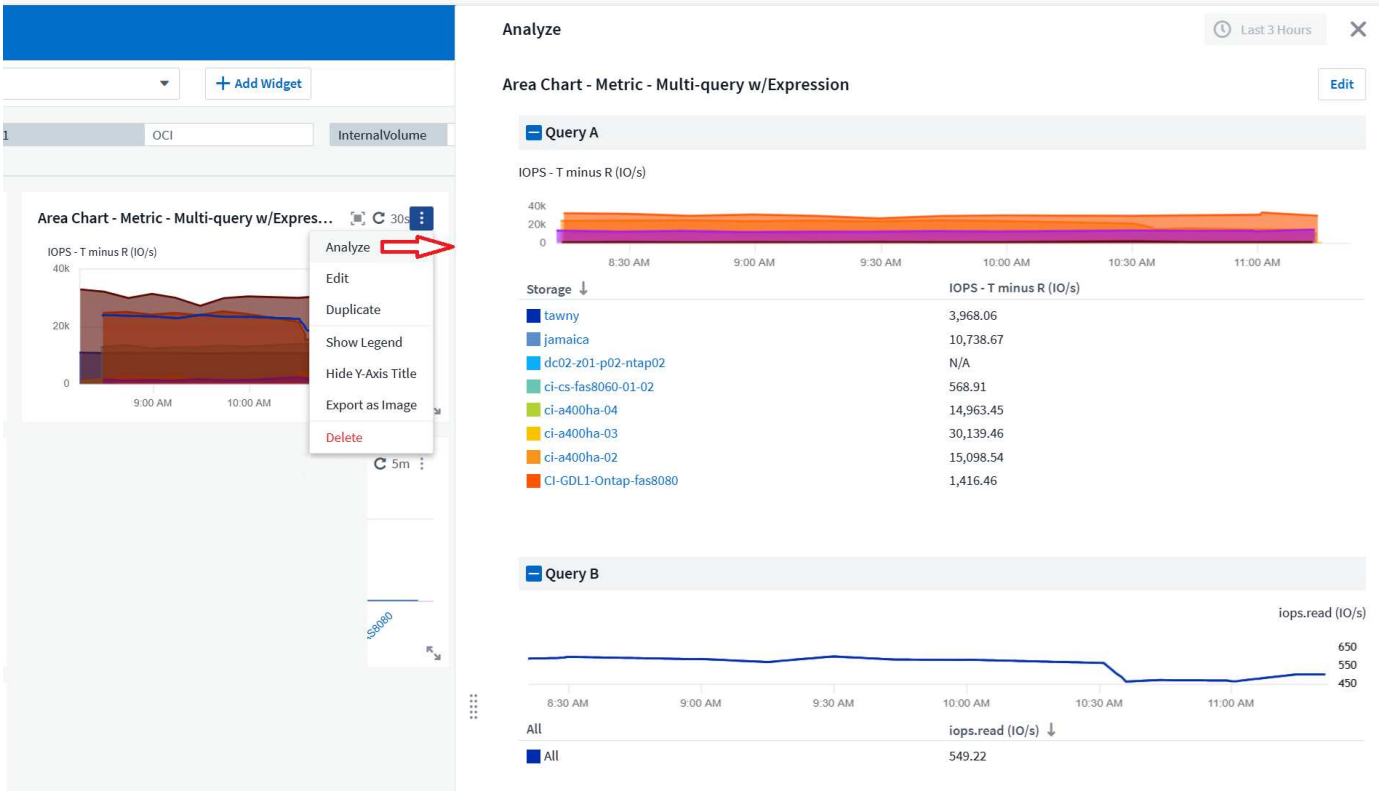
1. Visualizza e gestisci i gruppi con *GET /rest/v1/cloudsecure/activities/groups*.
2. Metti in pausa e riprendi i raccoglitori di dati con *POST /rest/v1/cloudsecure/collectors/{collector-uuid}/status*

Inoltre, i controlli delle autorizzazioni dei ruoli di Workload Security sono ora ancora più sicuri. Grazie al miglioramento della sicurezza, alcuni utenti esistenti potrebbero riscontrare problemi di autorizzazione quando aggiungono un raccoglitore. Confermare i permessi dell'utente seguendo le istruzioni nel"documentazione" .

Agosto 2025

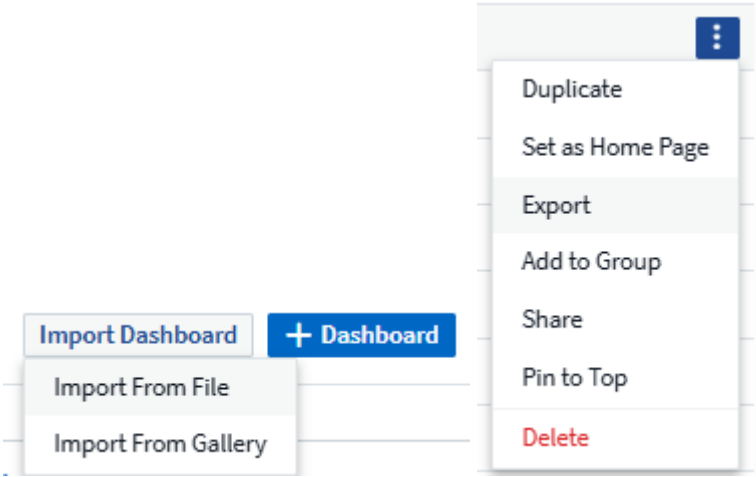
Dati widget mirati a portata di mano

La nuova funzionalità **Analizza** presente nella maggior parte dei widget consente di analizzare più da vicino i dati di un widget alla volta. Basta fare clic sul pulsante "Analizza" su un widget per aprire una vista dettagliata, in cui è possibile esplorare in modo interattivo i dati sottostanti e ingrandire per ottenere informazioni più approfondite, senza uscire dal contesto della dashboard.



Dashboard di esportazione e importazione

Se gestisci più tenant e hai sviluppato una dashboard utile, puoi esportare la dashboard e importarla in un altro tenant.



Integrazione cloud avanzata: supporto Google Cloud NetApp Volumes (GCNV)

- Google Cloud NetApp Volumes* (GCNV) è ora pienamente supportato come raccoglitore di dati in DII, completando il nostro ecosistema per il monitoraggio del cloud ibrido. Ottieni visibilità sugli oggetti di archiviazione critici come organizzazioni, pool e volumi nell'intera infrastruttura. Ora puoi monitorare tutti i tuoi ambienti di archiviazione, in locale o nel cloud, da un'unica piattaforma.

Monitoraggio StorageGRID migliorato

La raccolta dei log StorageGRID è ora abilitata per impostazione predefinita, fornendo dati di monitoraggio degli eventi a DII; inoltre, abbiamo ampliato il monitoraggio di StorageGrid con oltre 50 avvisi predefiniti, monitoraggio degli eventi in tempo reale e nuove dashboard per semplificare le complesse operazioni di Storage Grid. Rimani al passo con i problemi grazie a informazioni più approfondite sulle policy del traffico e sulle prestazioni dei bucket.

Supporto del sistema operativo

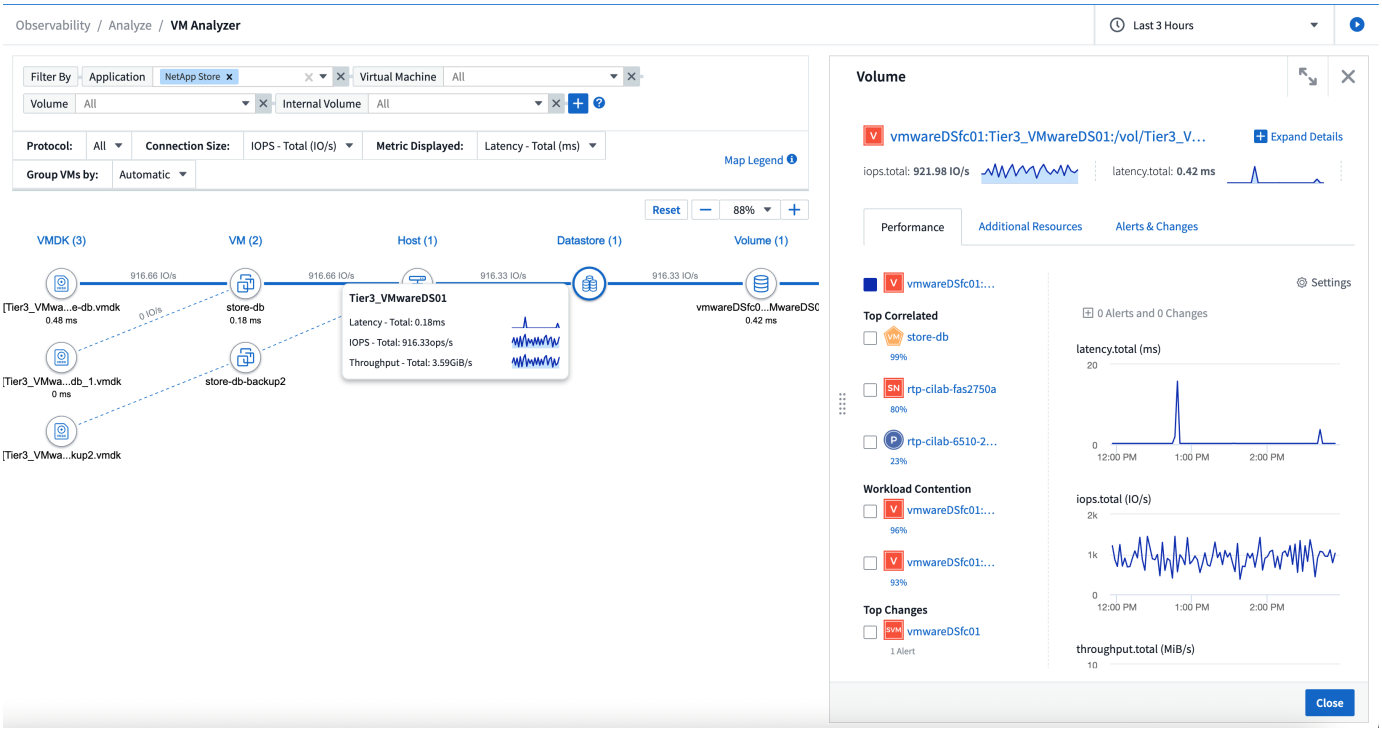
Oltre a quelli, i seguenti sistemi operativi sono ora supportati con Data Infrastructure Insights Acquisition Units"già supportato" :

- AlmaLinux (64 bit) 10
- Red Hat (64 bit) 10
- Rocky (64 bit) 9.6

Giugno 2025

VM Analyzer: visibilità olistica da VM a storage e risoluzione dei problemi

La funzionalità **VM Analyzer** di DII fornisce una visione completa ed end-to-end degli ambienti virtualizzati. VM Analyzer semplifica la risoluzione dei problemi mappando l'intero percorso dalle macchine virtuali allo storage, consentendo agli utenti di individuare rapidamente i problemi di prestazioni su dischi virtuali, VM, host, datastore, volumi e storage. Grazie a una visualizzazione intuitiva della topologia, al filtraggio e alle metriche dettagliate delle prestazioni, gli amministratori possono identificare facilmente i colli di bottiglia, analizzare gli squilibri del traffico e ottimizzare le prestazioni complessive dello storage.



Supporto del sistema operativo

Oltre a quelli, i seguenti sistemi operativi sono ora supportati con Data Infrastructure Insights Acquisition Units"già supportato" :

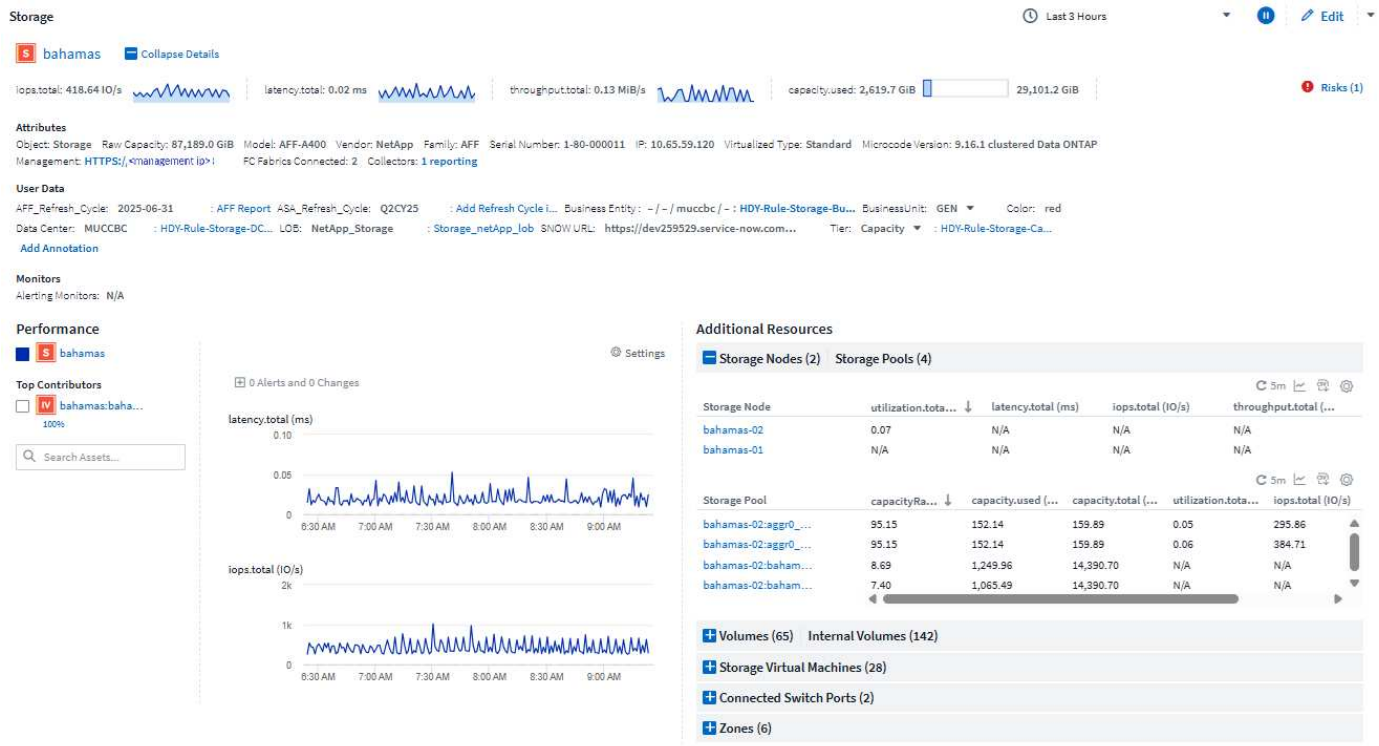
- Debian (64 bit) 12
- Oracle Enterprise Linux (64 bit) 9.6
- Red Hat (64 bit) 9,6

Maggio 2025

Le nuove landing page ti mantengono aggiornato

Le landing page riprogettate presentano tutto ciò di cui hai bisogno: dati riepilogativi, grafici delle prestazioni, correlazioni, avvisi e modifiche, nonché risorse chiave, in un'unica visualizzazione.

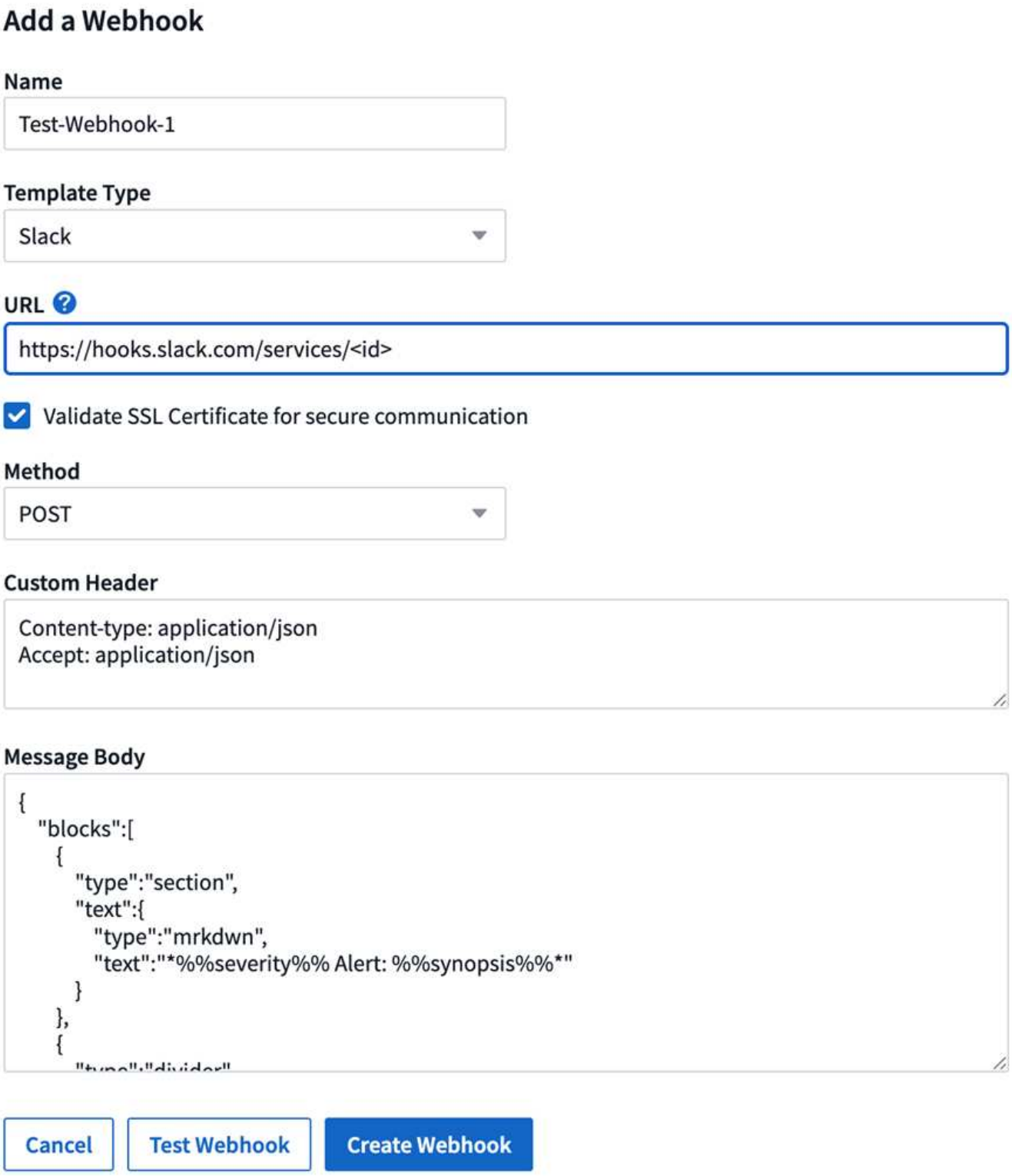
Ora puoi risolvere i problemi più velocemente e rimanere aggiornato, senza dover passare da una scheda all'altra o perdere il contesto.



Miglioramenti della sicurezza del carico di lavoro

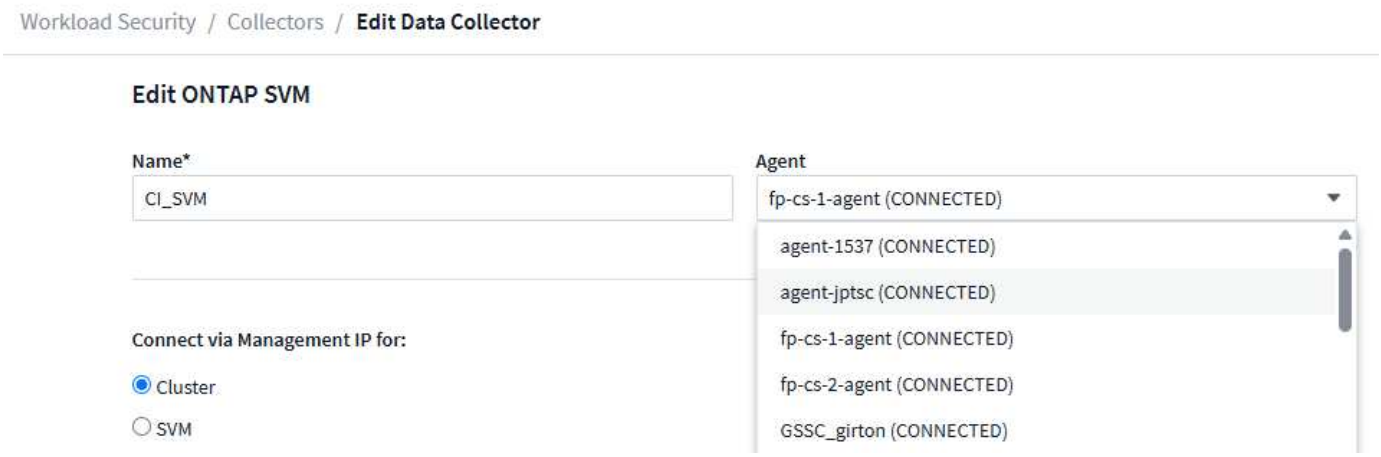
Webhook ora disponibili per gli avvisi di sicurezza del carico di lavoro

Workload Security ora supporta notifiche webhook pronte all'uso per strumenti come Slack, PagerDuty, Teams e altri. Inoltre, offriamo modelli personalizzabili che consentono di personalizzare il messaggio o di integrarlo con qualsiasi altra applicazione SIEM o di terze parti. Invia gli avvisi critici direttamente ai tuoi flussi di lavoro di sicurezza esistenti, in modo che il tuo team possa indagare e rispondere più rapidamente.



Migrare i collettori di sicurezza del carico di lavoro tra gli agenti

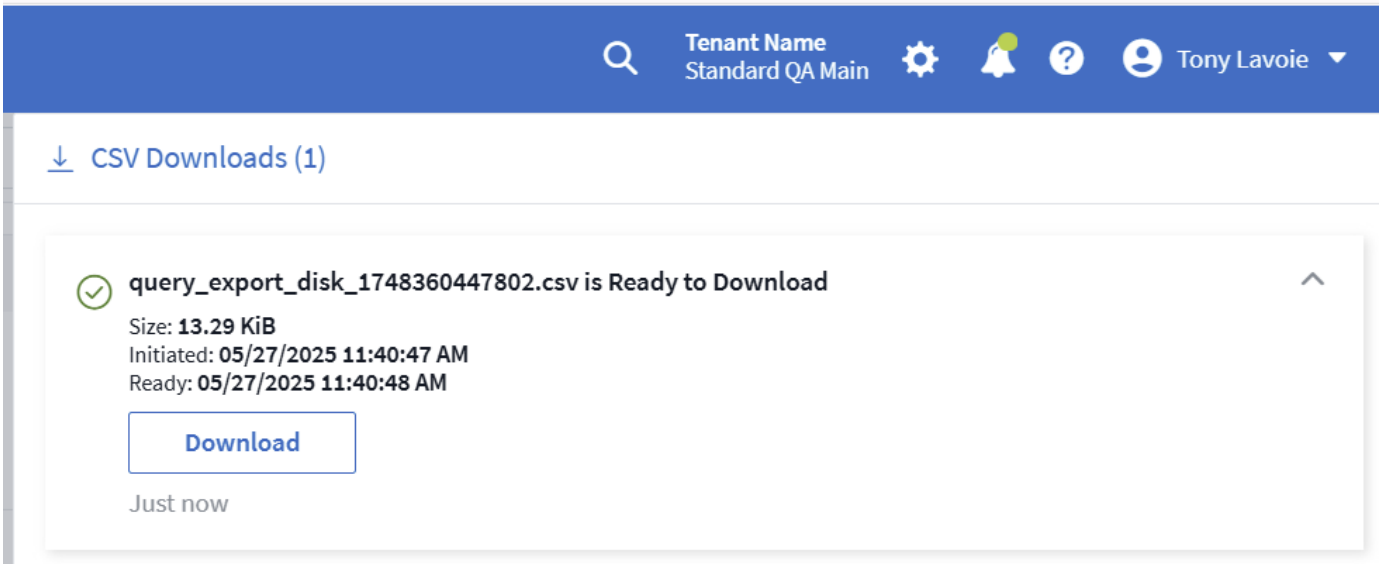
È possibile migrare facilmente un collettore Workload Security da un agente all'altro, consentendo un efficiente bilanciamento del carico dei collettori tra gli agenti. La migrazione è semplice: basta modificare il raccoglitore e selezionare l'agente di destinazione dall'elenco.



Esportazione asincrona .CSV

L'esportazione dei dati in formato .CSV può richiedere da pochi secondi a diverse ore, a seconda della quantità di dati da esportare. Ora Data Infrastructure Insights esporta i dati in modo asincrono, così puoi continuare a lavorare mentre il file .CSV viene compilato.

Visualizza le tue esportazioni .CSV selezionando l'icona "Campana" nella barra degli strumenti in alto a destra.



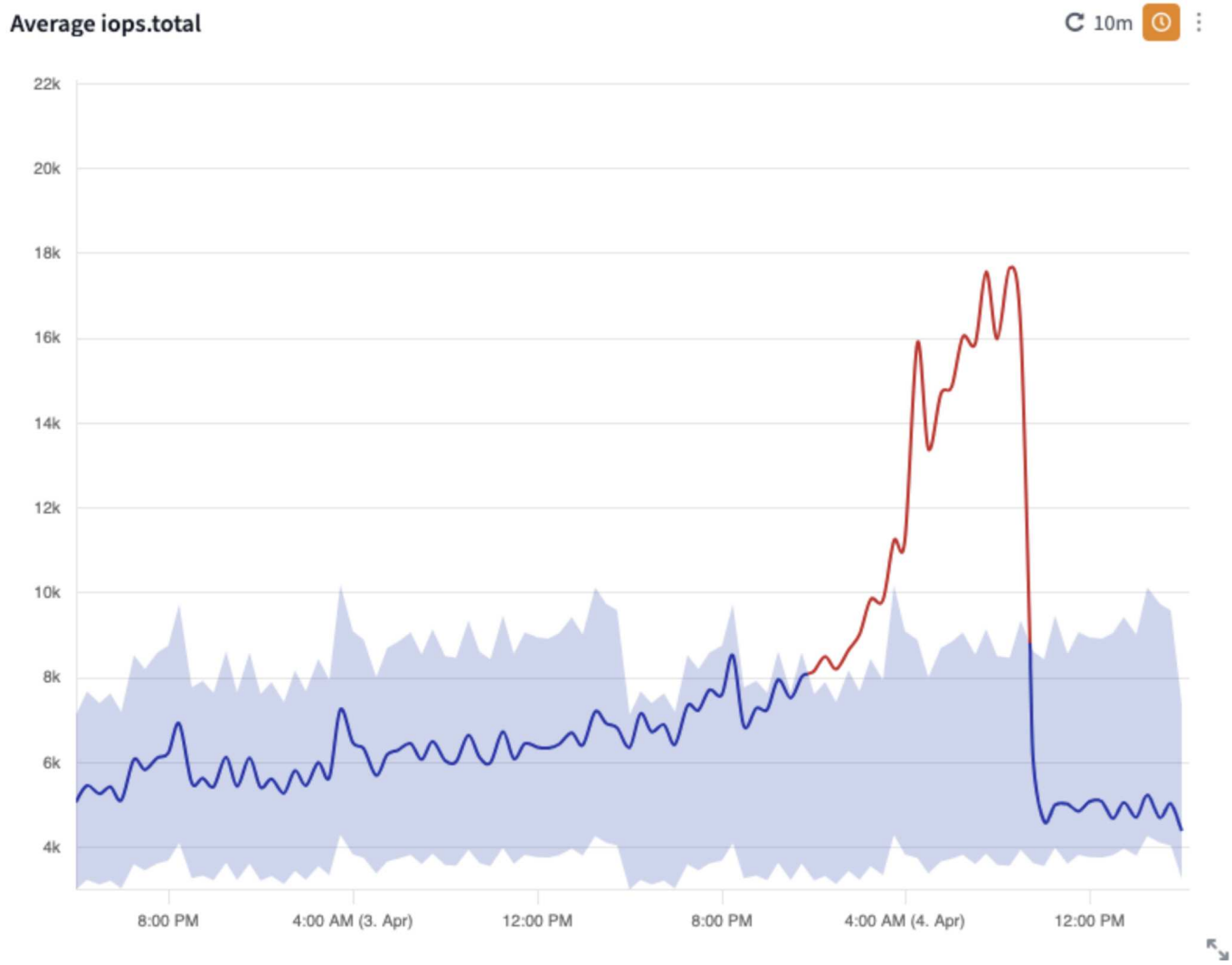
Aprile 2025

Limiti di anomalia basati su ML nei widget di linea per la risoluzione proattiva dei problemi

Per risolvere i problemi di prestazioni con i widget dei grafici a linee o spline, ora puoi visualizzare i limiti del comportamento previsto accanto alle metriche effettive, consentendoti di distinguere tra tendenze metriche normali e anomale.

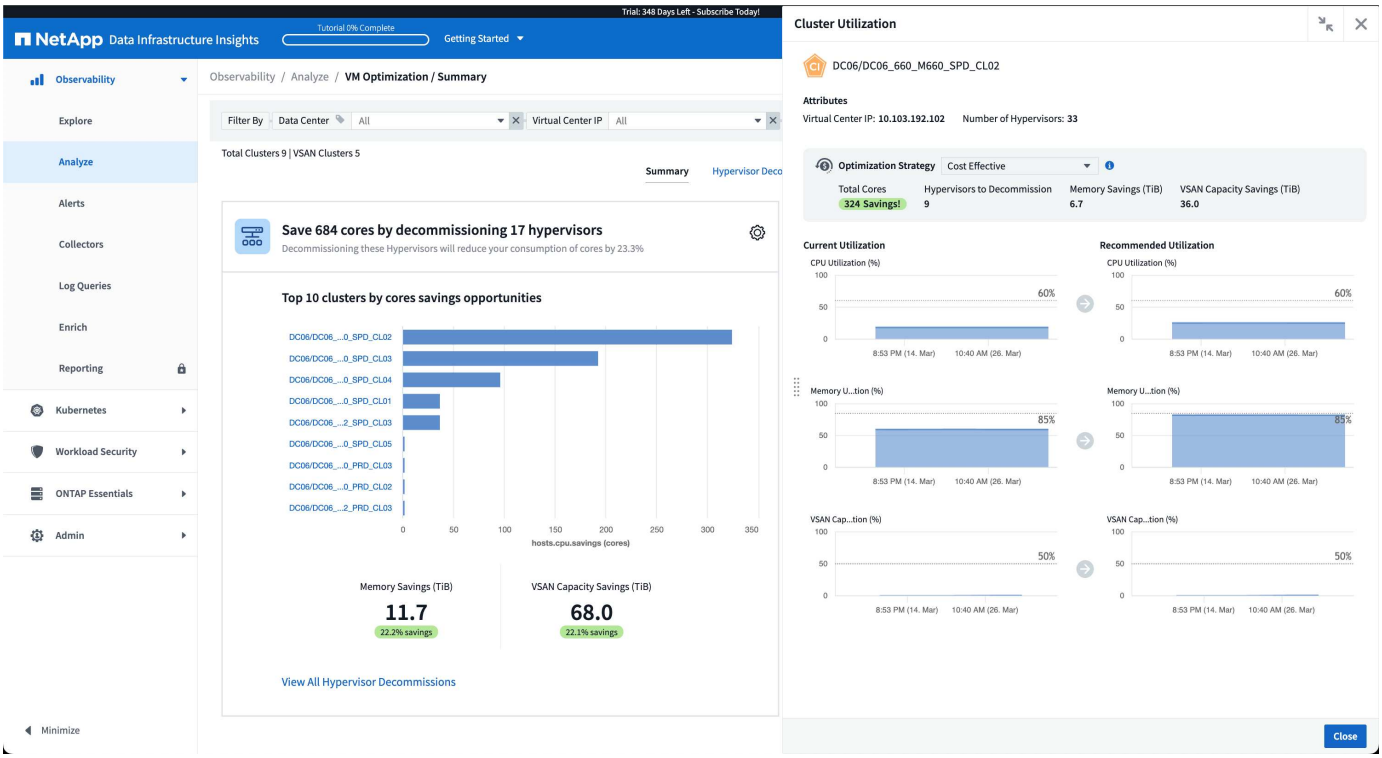
L'apprendimento automatico DII con analisi dei dati stagionali stabilisce soglie intelligenti basate su modelli storici. Quando le metriche si discostano dagli intervalli previsti, il sistema le evidenzia come anomalie,

consentendo una rapida identificazione dei problemi, riducendo il tempo medio di risoluzione e affrontando i problemi prima che incidano sulle operazioni.



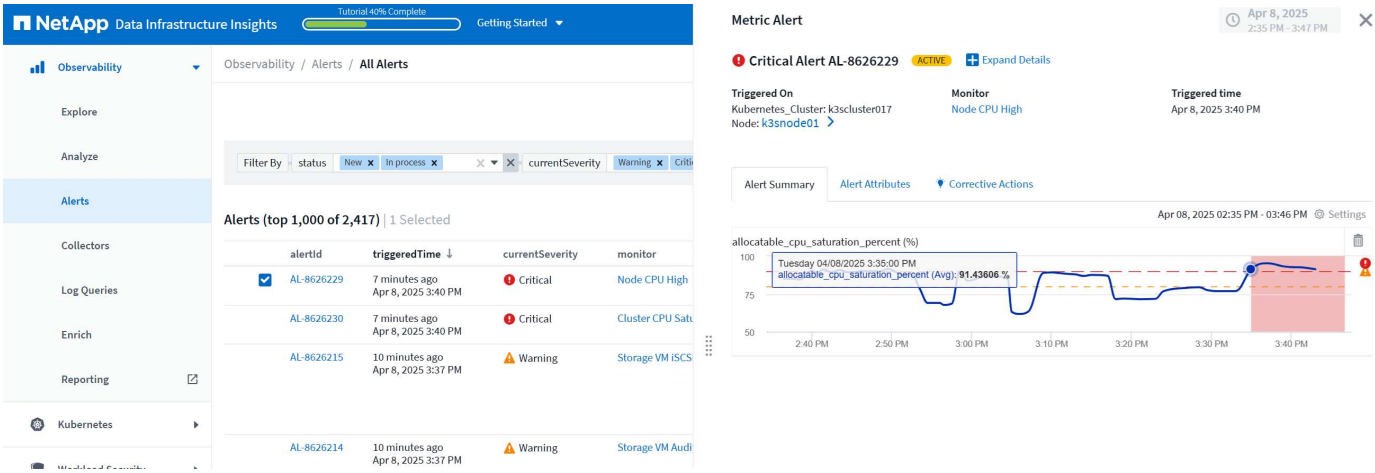
Ottimizza i costi VMware con il supporto di archiviazione VSAN

La nostra funzionalità di ottimizzazione delle VM ora include il supporto per gli ambienti VMWare con storage VSAN. Oltre all'utilizzo di CPU e memoria, l'analisi ora prende in considerazione l'archiviazione VSAN locale per i consigli di recupero, aiutandoti a ridurre ulteriormente i costi di licenza.



Dettagli degli avvisi a portata di mano

Grazie al nuovo pannello scorrevole, analizzare gli avvisi è più facile che mai. Seleziona un avviso per visualizzarne i dettagli e passa facilmente da un avviso all'altro senza perdere il segno durante l'analisi dei problemi.



Esportazione asincrona di analisi forense della sicurezza del carico di lavoro

L'esportazione dei dati forensi può richiedere da pochi secondi a diverse ore, a seconda della quantità di dati da esportare. Workload Security esporta tali dati in modo asincrono, così puoi continuare a lavorare mentre il file .CSV viene compilato.

Notifiche del Data Collector raggruppate in regole

Se hai configurato le notifiche sui raccoglitori di dati, a partire dal 15 aprile tali notifiche verranno gestite nelle Regole di notifica, con un'unica regola per i raccoglitori che hanno destinatari identici. I collezionisti con

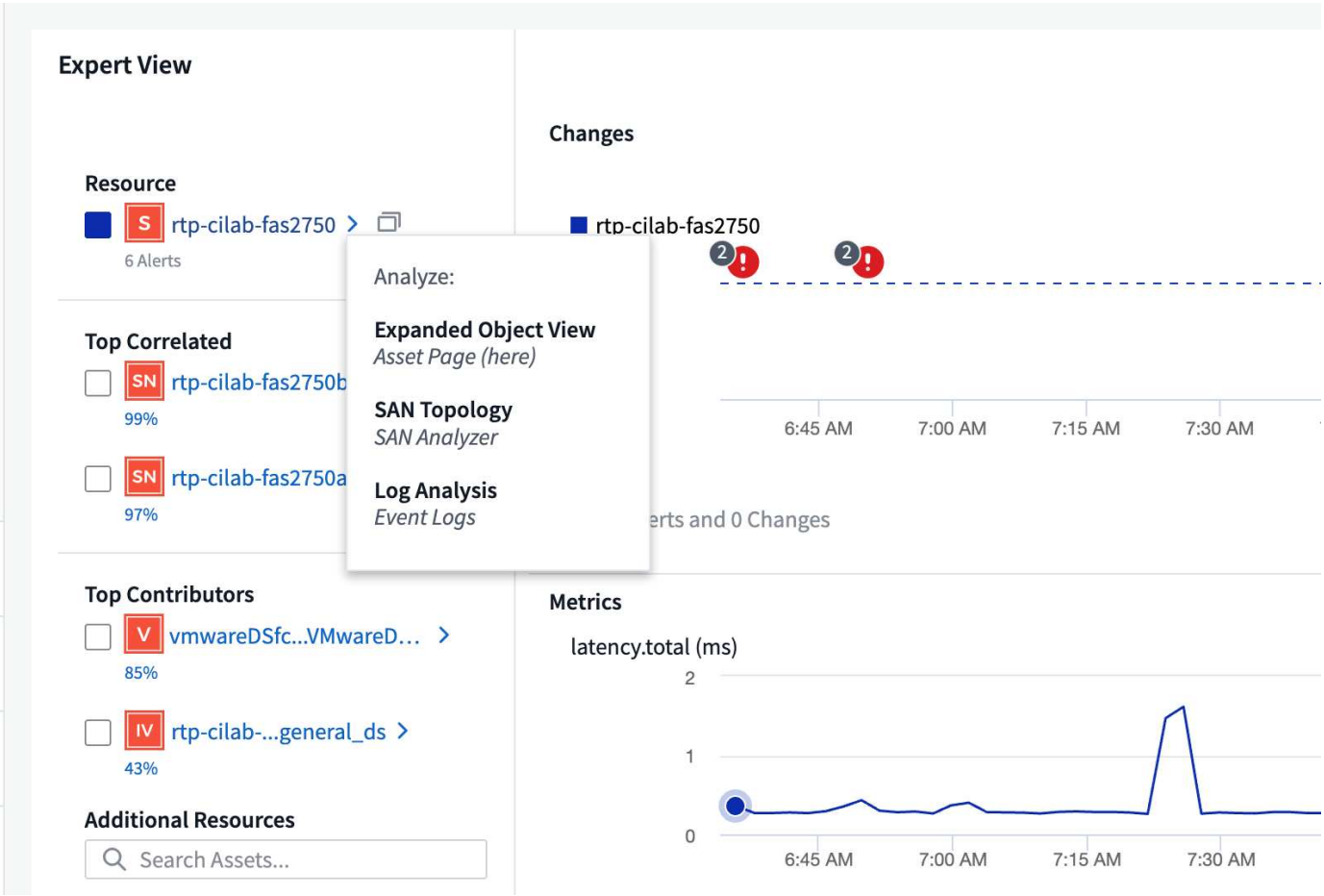
destinatari diversi avranno regole separate. Le notifiche del collettore esistenti vengono migrate alle regole di notifica.

Marzo 2025

Navigazione contestuale migliorata per una gestione efficiente delle infrastrutture

Risparmia tempo sfruttando Data Infrastructure Insights per l'eccellenza operativa. Stiamo aggiungendo collegamenti al menu contestuale che consentono di passare direttamente da qualsiasi oggetto alla landing page delle risorse per ottenere informazioni sulle prestazioni del dispositivo, a SAN Analyzer per la visualizzazione della topologia di rete, ai registri per la consapevolezza operativa o a Change Analyzer per la gestione della configurazione.

Grazie all'accesso immediato ai dati chiave in più viste, è possibile comprendere più chiaramente e più rapidamente le relazioni tra gli oggetti. Questo flusso di lavoro semplificato accelera il processo decisionale e la risoluzione dei problemi, facendoti risparmiare tempo e migliorando le tue capacità di analisi complessive.



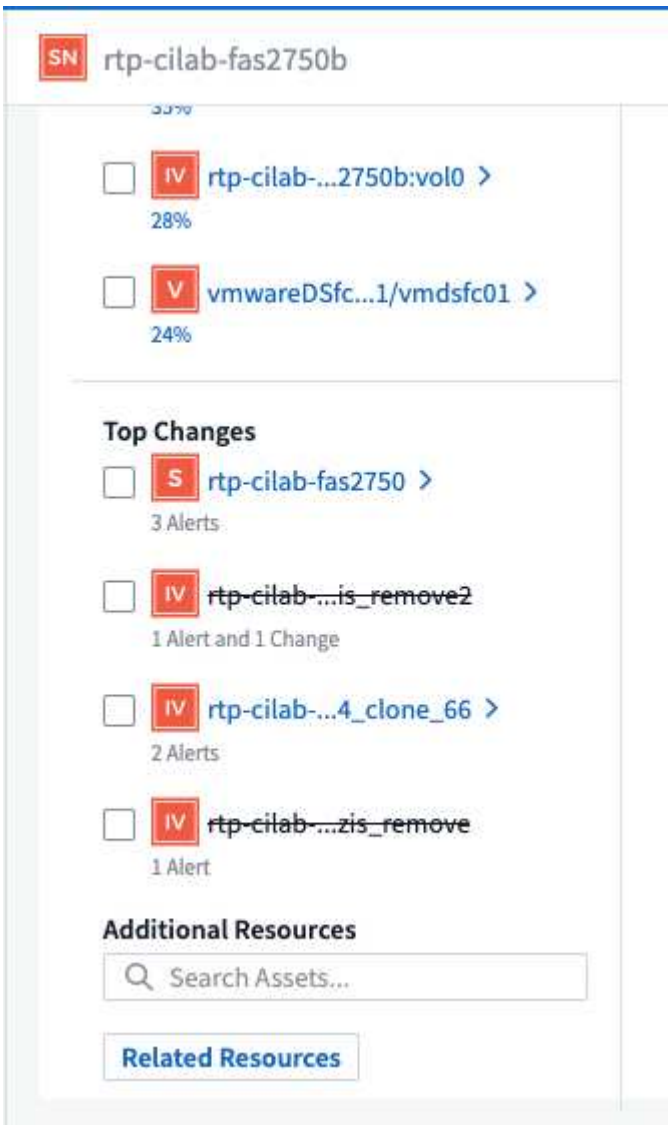
Conserva la cronologia delle risorse rimosse

La nostra funzionalità avanzata di modifica dell'infrastruttura ora conserva la cronologia delle risorse rimosse, come qtree e volumi che sono stati spostati e non sono più disponibili.

Ti manca qualcosa nel tuo puzzle di risoluzione dei problemi? Non più! Vedrai tutto, compresi gli oggetti eliminati contrassegnati con una barra, fornendoti un contesto completo anche dopo la rimozione delle risorse,

assicurandoti di non perdere mai elementi critici derivanti da modifiche passate o avvisi lungo il percorso end-to-end.

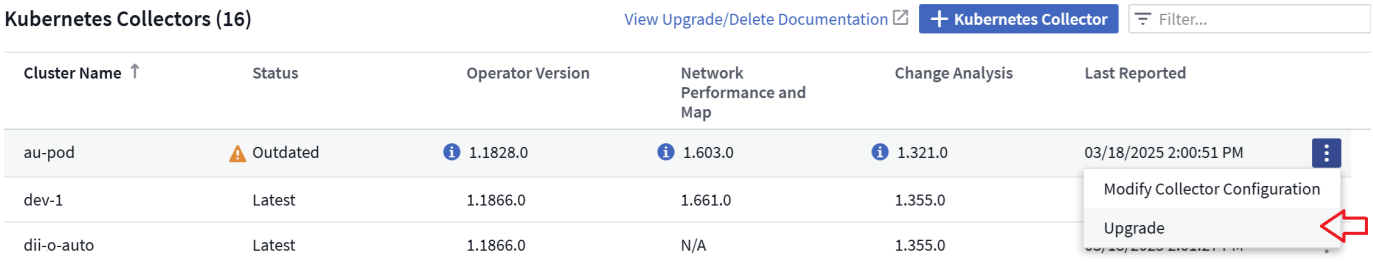
Il risultato? Tempi di risoluzione più rapidi e decisioni infrastrutturali più affidabili, anche quando le risorse in questione non esistono più.



Aggiornamento tramite pulsante dell'operatore Kubernetes

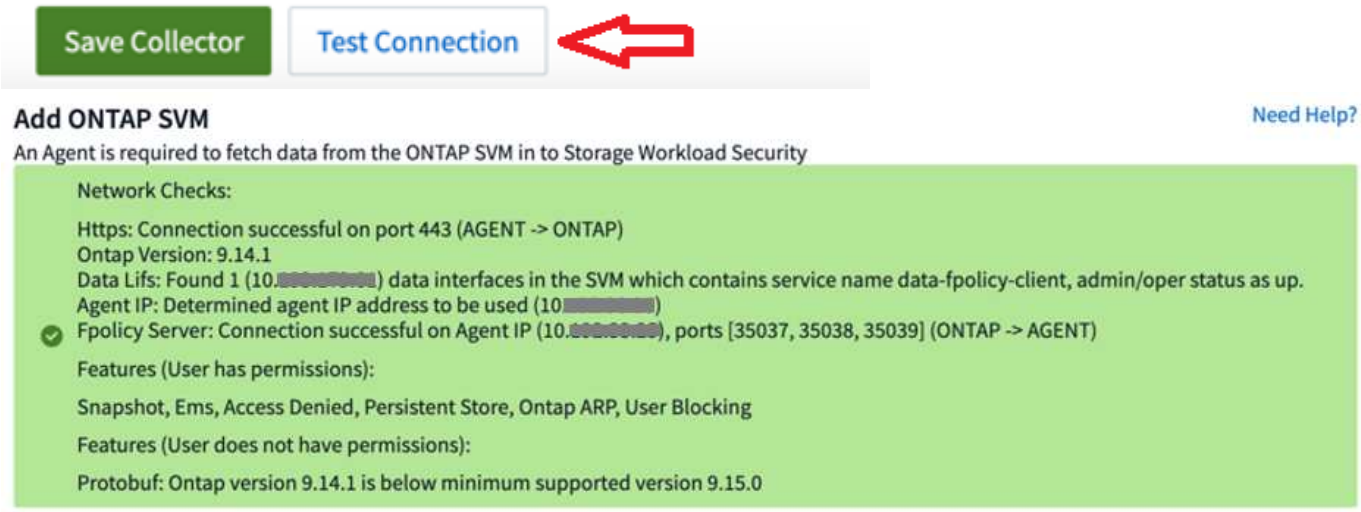
Vuoi essere sicuro di avere la versione più recente di Kubernetes Operator? Aggiorna l'operatore su richiesta dal menu del cluster DII Kubernetes Collectors. Basta selezionare Aggiorna dal menu e l'operatore verificherà le firme delle immagini, catturerà un'istantanea dell'installazione corrente ed eseguirà l'aggiornamento.

L'aggiornamento tramite pulsante è una funzionalità opzionale e la sua attivazione può essere gestita per ogni cluster.



Test di connettività per i collettori di dati di sicurezza del carico di lavoro di archiviazione

La funzionalità di test della connettività ha lo scopo di aiutare gli utenti finali a identificare le cause specifiche dei guasti durante la configurazione dei raccoglitori di dati in Data Infrastructure Insights (DII) Workload Security. Ciò consente agli utenti di correggere autonomamente i problemi relativi alla comunicazione di rete o ai ruoli mancanti.



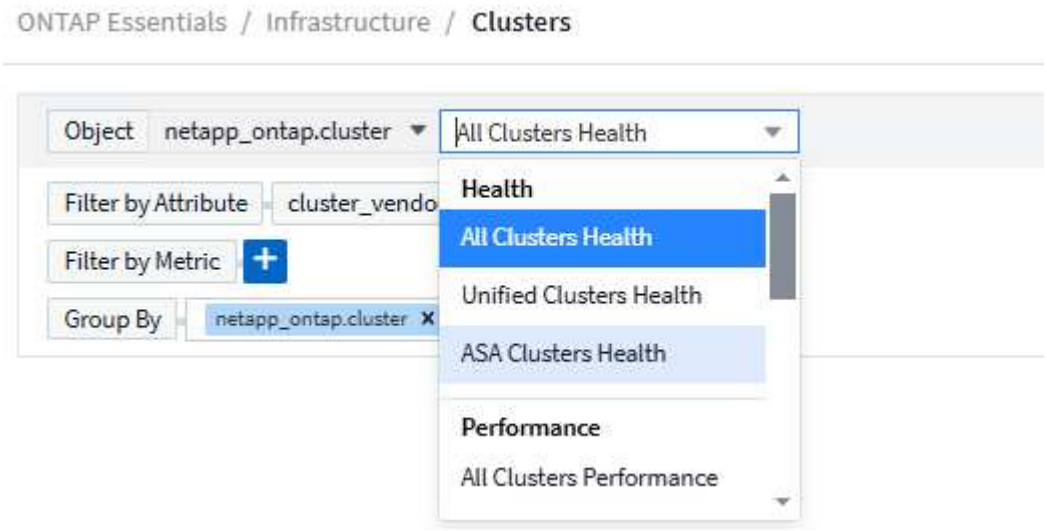
Supporto del sistema operativo

Oltre a quelli, i seguenti sistemi operativi sono ora supportati con Data Infrastructure Insights Acquisition Units"già supportato" :

- AlmaLinux 9.5
- Debian (64 bit) 11
- OpenSUSE Leap 15.6
- Oracle Enterprise Linux (64 bit) 8.9, 8.10, 9.5
- Red Hat (64 bit) 8.9, 8.10, 9.5
- Rocky 9.5
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Server 24.04 LTS

Febbraio 2025

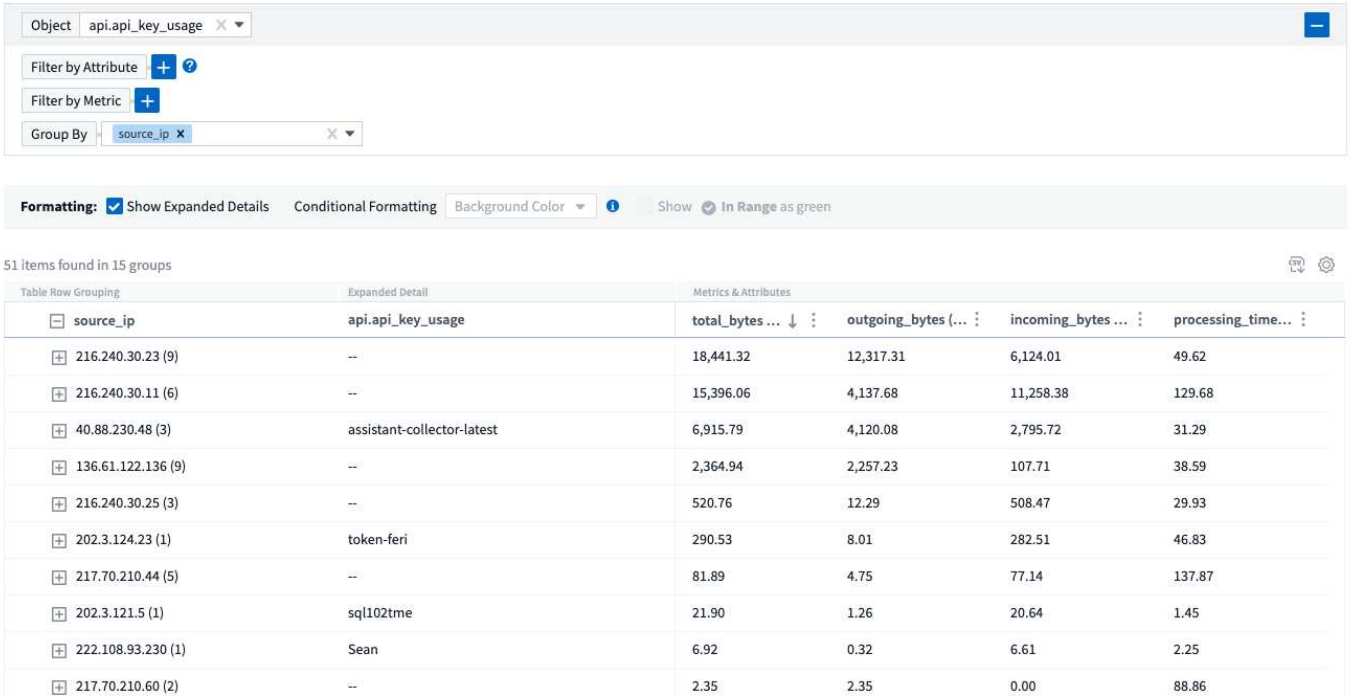
ONTAP Essentials ora include la gestibilità immediata per l'ultima generazione di"ASA" dispositivi. Ciò include SAN Analyzer per topologie VM-to-LUN di carichi di lavoro in esecuzione su ONTAP, ora disponibile anche con supporto NetApp come parte di Data Infrastructure Insights Basic Edition.



Monitoraggio dell'utilizzo dell'API DII: migliora la sicurezza e l'efficienza

Rafforza la tua sicurezza e semplifica la gestione delle risorse con il monitoraggio avanzato dell'utilizzo delle API REST, disponibile per gli utenti amministratori. Grazie al monitoraggio dell'utilizzo delle API puoi vedere quali token API vengono utilizzati, da quali indirizzi IP e il volume di traffico che generano. Collegando i token a specifici indirizzi IP e livelli di utilizzo, otterrai informazioni approfondite sull'accesso al sistema e sulle tendenze di utilizzo, ottenendo il controllo necessario per mantenere un ambiente sicuro ed efficiente e garantire il regolare svolgimento delle operazioni.

Per visualizzare l'utilizzo dell'API, vai su **Osservabilità > Amministrazione > Accesso API** e seleziona *Visualizza utilizzo API*. Si noti che questa API è disponibile solo per le API DII Observability; non si applica a Workload Security.



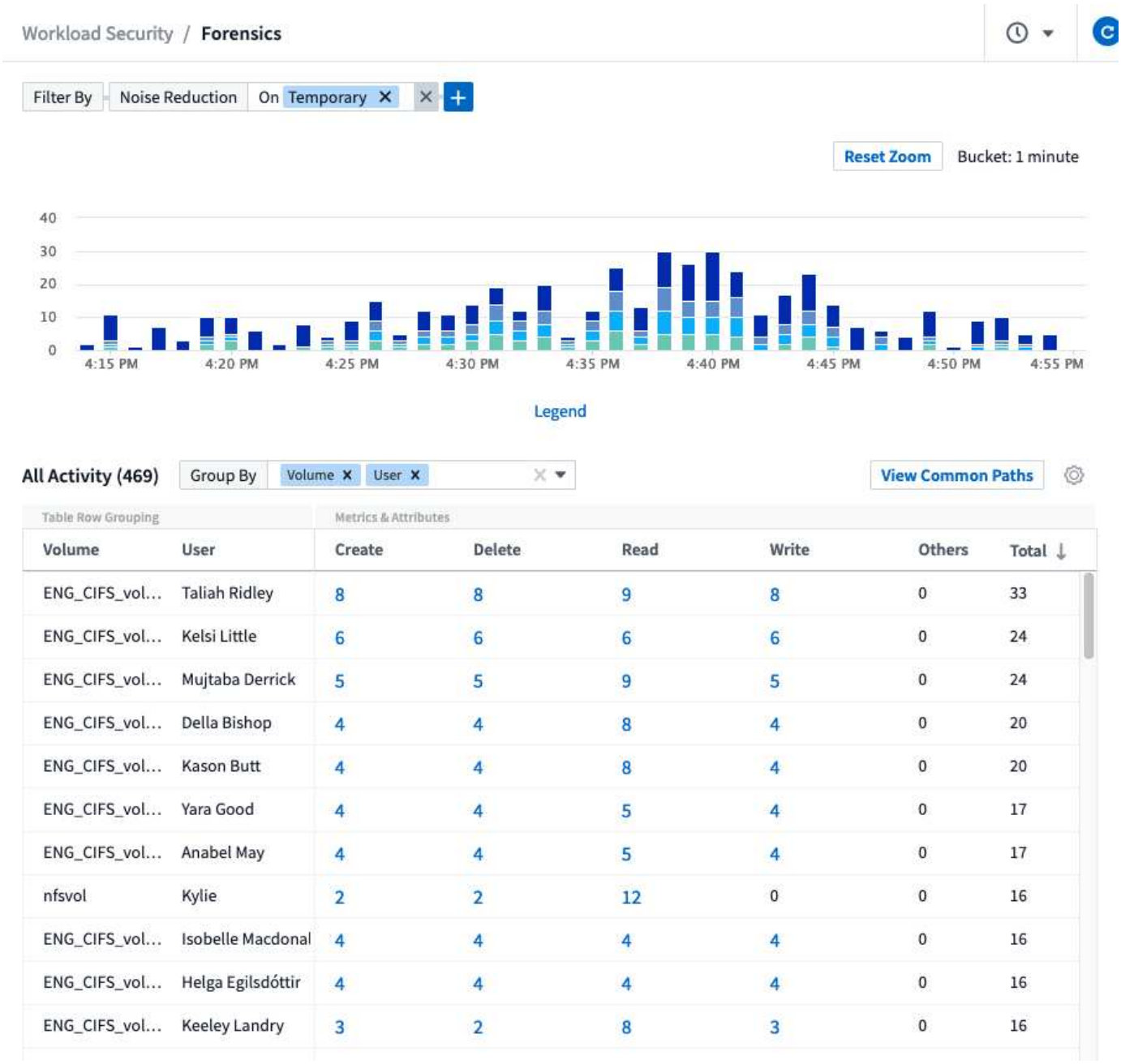
API di sicurezza del carico di lavoro per limitare gli utenti

È stata aggiunta una nuova API per gestire le restrizioni utente in Workload Security. Con l'API puoi bloccare o sbloccare un utente oppure modificare la durata del suo accesso limitato. Consultare la pagina Amministrazione > Accesso API > Documentazione API per l'API *cloudsecure_actions.block*.

Gennaio 2025

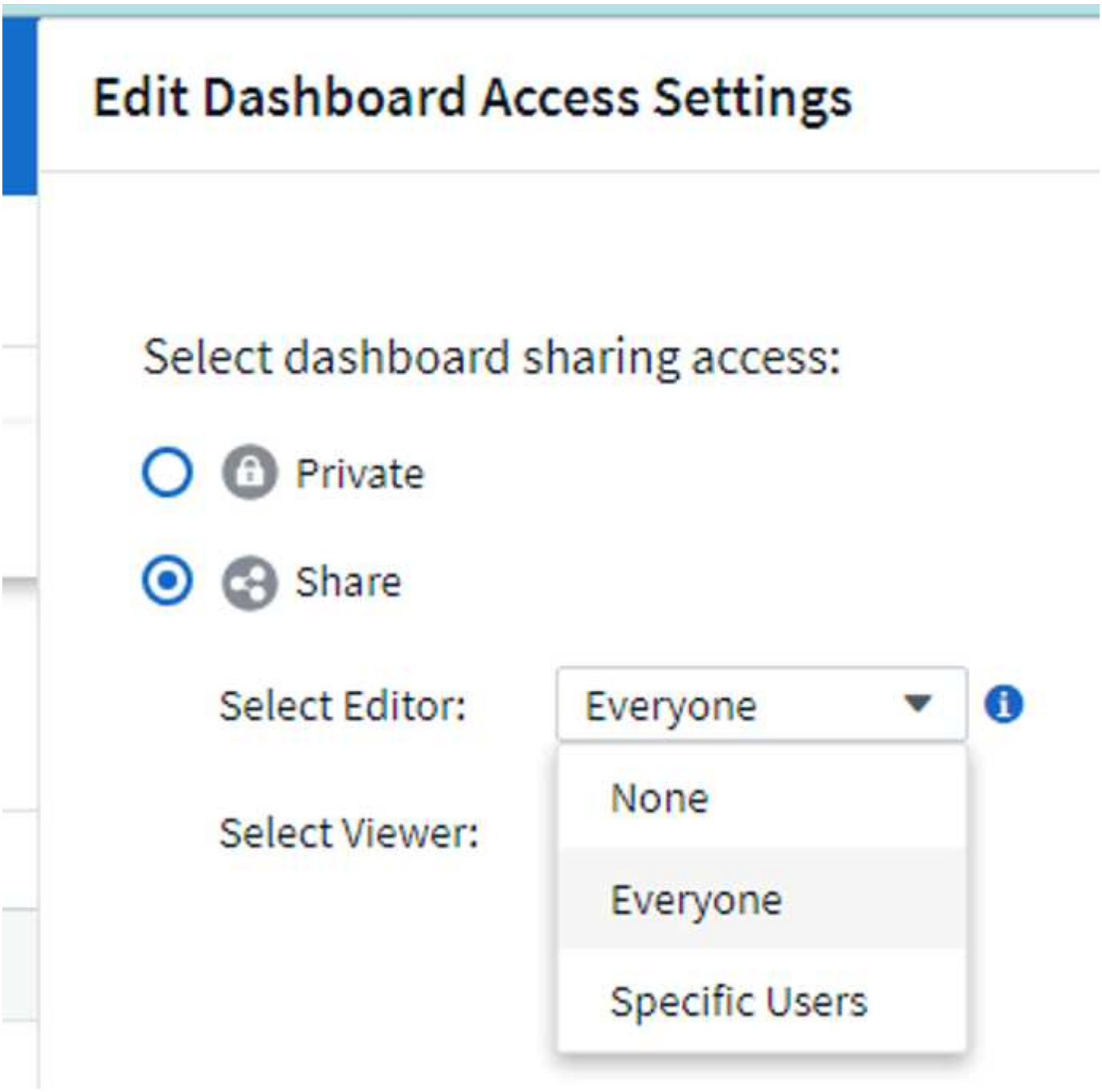
Gestire proattivamente il rischio con Forensics Grouping

Vi presentiamo la nostra ultima funzionalità progettata per migliorare le vostre capacità di sicurezza e gestione delle risorse! Grazie alla funzionalità avanzata di raggruppamento e al supporto gerarchico di raggruppamento multiplo, ora puoi identificare facilmente gli utenti che hanno avuto accesso a cartelle specifiche, determinare gli utenti e le condivisioni più attivi e gestire in modo proattivo i rischi monitorando gli indirizzi IP dei client attivi. Ottimizza l'utilizzo dello spazio di archiviazione e della larghezza di banda individuando i file e le cartelle a cui si accede più spesso e ottieni un maggiore controllo sull'accesso al sistema identificando gli utenti.



Controllo degli accessi alla dashboard

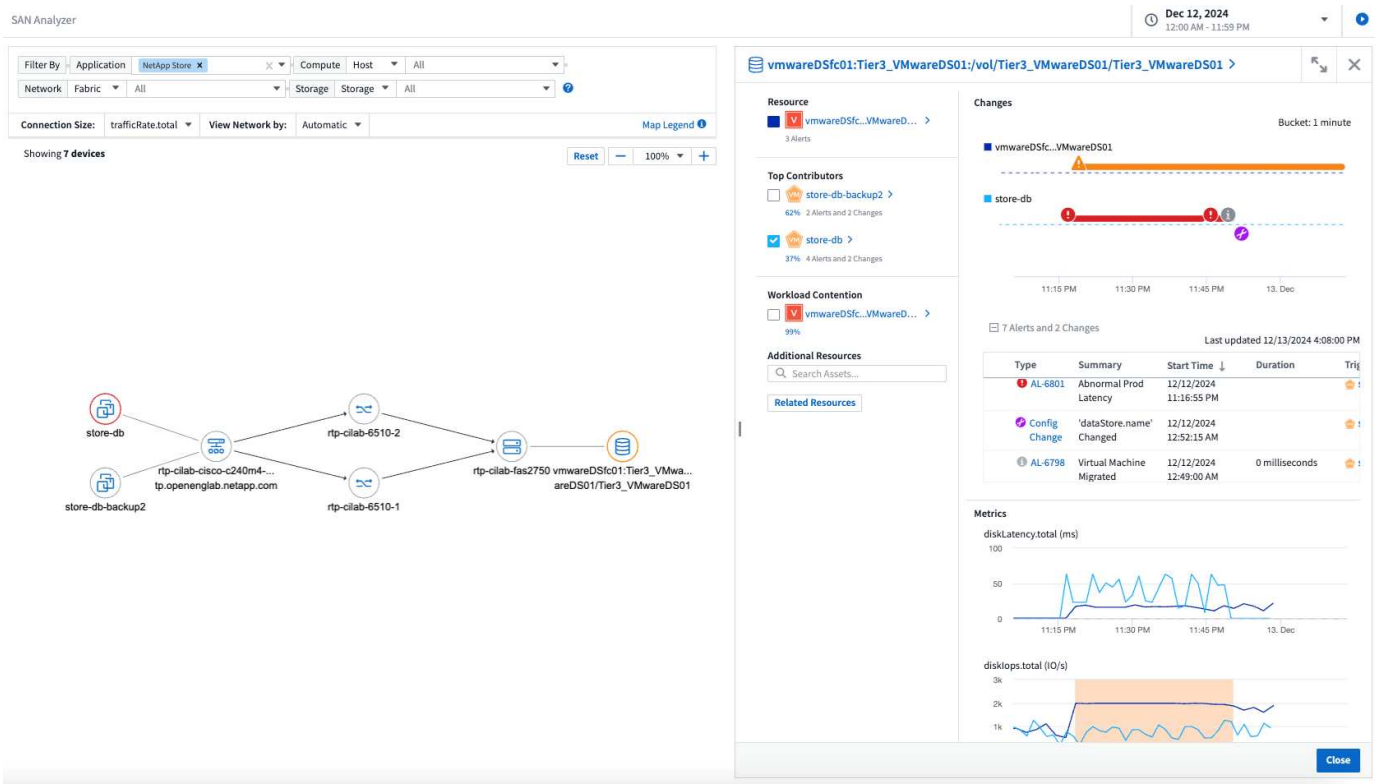
Data Infrastructure Insights ora ti offre un maggiore controllo sull'accesso alle dashboard che crei. Puoi scegliere chi può modificare i tuoi grafici. Puoi controllare l'esposizione a informazioni potenzialmente sensibili. Stai ancora lavorando su una dashboard che non è pronta per la visibilità generale? Puoi mantenerlo privato finché non sarai pronto a condividerlo.



Dicembre 2024

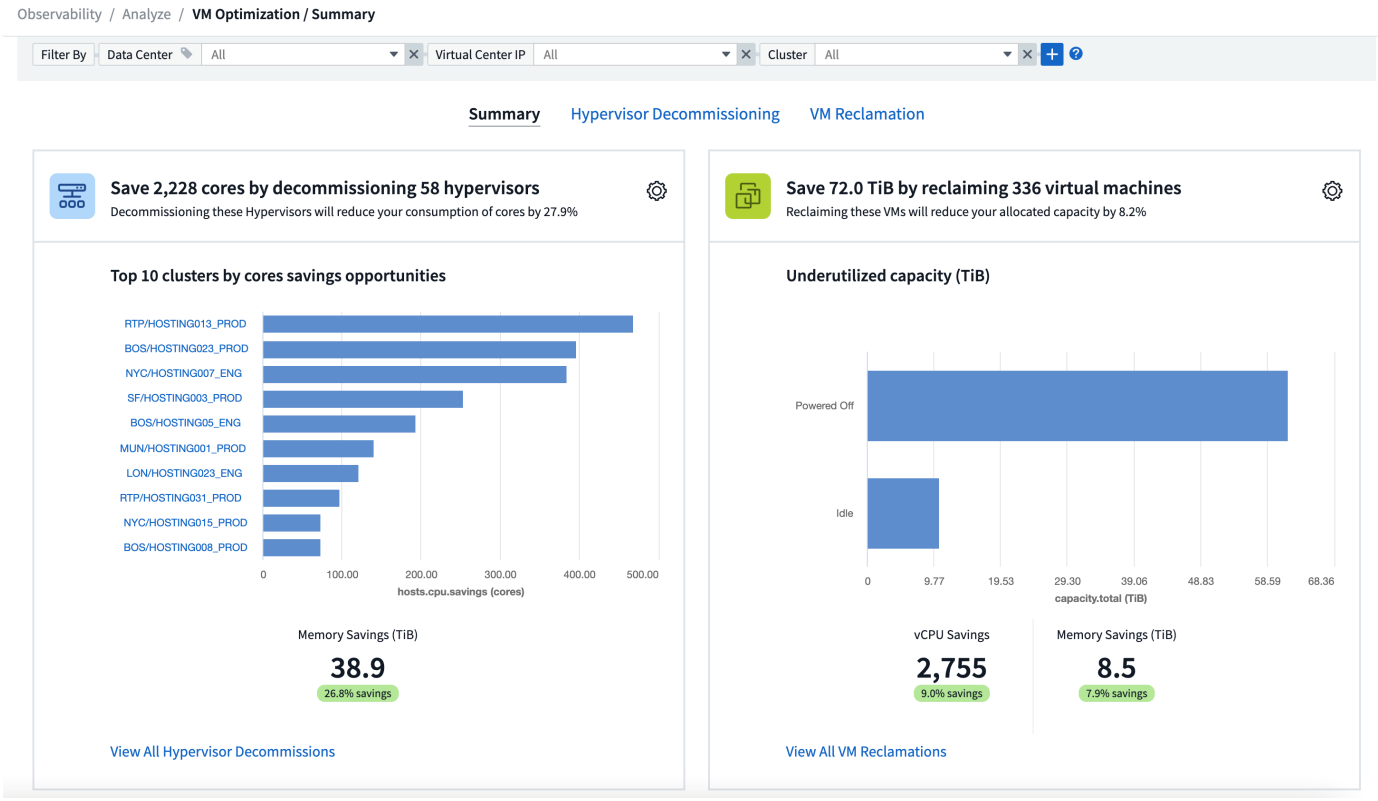
Presentazione di SAN Analyzer: visibilità migliorata per i carichi di lavoro a blocchi

La SAN svolge un ruolo cruciale nella gestione di carichi di lavoro vitali, ma la sua complessità può causare interruzioni significative e disagi per i clienti. Con **SAN Analyzer** di DII, la gestione della SAN diventa più semplice ed efficiente. Questo potente strumento offre visibilità end-to-end, mappando le dipendenze da VM/host a rete, LUN e storage. Grazie a una mappa topologica interattiva, SAN Analyzer consente di individuare i problemi, comprendere i cambiamenti e migliorare la comprensione del flusso di dati. Semplifica la gestione SAN in ambienti IT complessi con SAN Analyzer e aumenta la visibilità sui carichi di lavoro a blocchi.



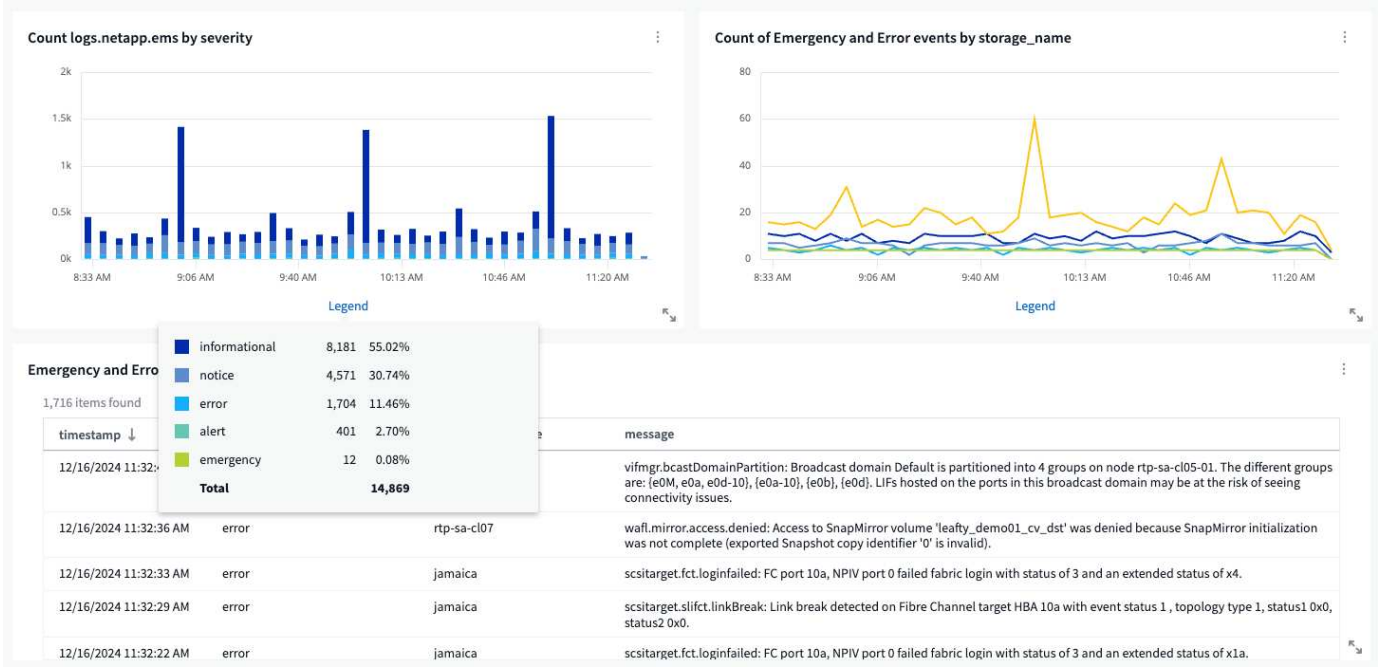
Ottimizza i costi delle VM con la dismissione intelligente degli host e il recupero delle VM

Data Infrastructure Insights ti aiuta a gestire i costi di infrastruttura e licenze analizzando il comportamento storico dell'ambiente e stabilendo previsioni a breve e lungo termine, generando raccomandazioni dettagliate per la dismissione dell'host e il recupero delle VM spente e inattive. Questi consigli ti aiutano a garantire la stabilità delle prestazioni, a liberare capacità inutilizzata e a ridurre l'allocazione di memoria e CPU.



Scopri informazioni dettagliate sui registri con il supporto dei grafici temporali e dei widget delle tabelle

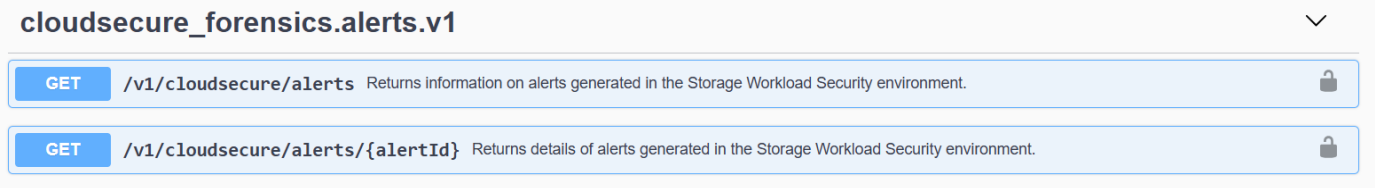
Ora puoi sfruttare i grafici temporali (a barre, a linee, ad aree) per identificare tendenze e modelli nei dati di registro, come errori ricorrenti o picchi di attività, ottenendo preziose informazioni sul comportamento del sistema nel tempo. Inoltre, grazie alle tabelle, ora è possibile includere i messaggi di registro direttamente nella dashboard, ottenendo una visualizzazione più completa dei dettagli del registro.



Novembre 2024

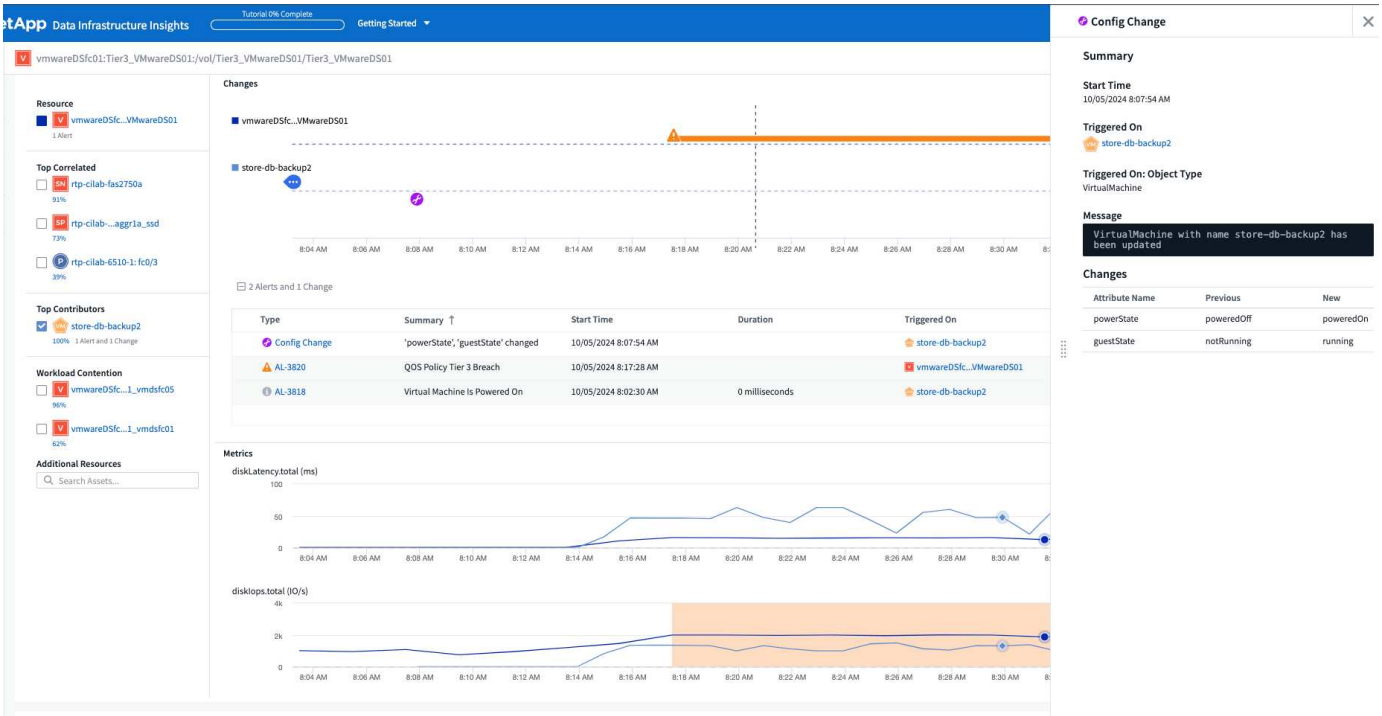
Nuova API per gli avvisi di sicurezza del carico di lavoro

Recupera i dettagli degli avvisi forensi con il nuovo Workload Security"API **cloudsecure_forensics.alerts"** .



Analizza le modifiche di configurazione nel tuo ambiente

Le modifiche alla configurazione sono una delle cause più comuni di problemi nell'IT moderno. Il nuovo Data Infrastructure Insights(DII)"analisi del cambiamento" La funzionalità ti consente di comprendere chiaramente i cambiamenti che causano problemi nel tuo ambiente. Accelera i tempi di risoluzione dei problemi mostrando tutte le modifiche ai dispositivi e ai componenti infrastrutturali correlati che potrebbero aver causato un problema. Inoltre, quando tu o il tuo team eseguite modifiche pianificate, potete convalidarle rapidamente e garantire che non si verifichino effetti imprevisti prima che i livelli di servizio ne risentano.



Supporto KubeVirt: monitora i carichi di lavoro delle macchine virtuali in esecuzione nel tuo cluster Kubernetes

DII ora supporta completamente KubeVirt, la soluzione di virtualizzazione nativa di Kubernetes utilizzata da piattaforme come OpenShift Virtualization e Harvester. Ottieni piena visibilità sulle metriche, sugli eventi, sulle modifiche alla configurazione e sul traffico di rete delle macchine virtuali e dei carichi di lavoro dei container all'interno dei tuoi cluster Kubernetes.

Ottobre 2024

Sblocca nuove informazioni con espressioni personalizzate nei monitor

Le espressioni consentono di eseguire operazioni aritmetiche nei monitor di rilevamento delle metriche e delle anomalie. Ecco alcuni esempi:

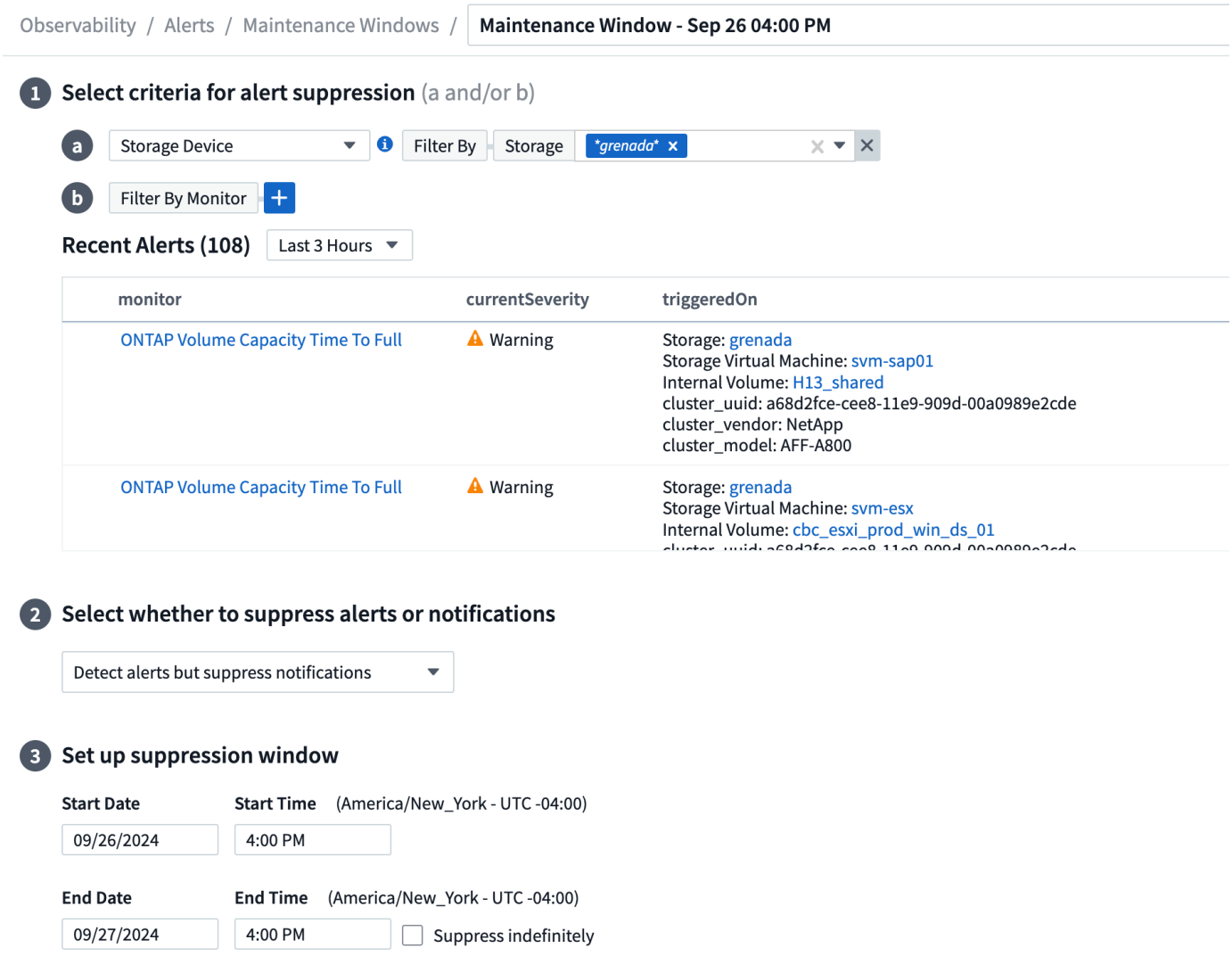
- Rapporto: IOPS/TB per rilevare dove vengono raggiunti i limiti del livello di servizio sui provider di archiviazione cloud.
- Percentuale: Utilizzata/Disponibile per calcolare l'utilizzo
- Aggregazione: combina più tipi di errori delle porte fisiche in un unico monitor
- Confronto: confronta l'attuale utilizzo delle risorse con il punto di headroom ottimale per identificare le risorse che non funzionano a piena capacità.

Ridurre al minimo le interruzioni degli avvisi durante il periodo di manutenzione

Le finestre di manutenzione consentono di sopprimere le notifiche di avviso durante i periodi di manutenzione programmata, aiutandoti a evitare interruzioni non necessarie.

Con le finestre di manutenzione puoi pianificare specifici periodi di manutenzione durante i quali le notifiche di avviso vengono soppresse per gli oggetti e le metriche che scegli. Ad esempio, è possibile sopprimere le notifiche di avviso attivate da specifici sistemi di archiviazione quando tali sistemi di archiviazione sono in un periodo di aggiornamento pianificato.

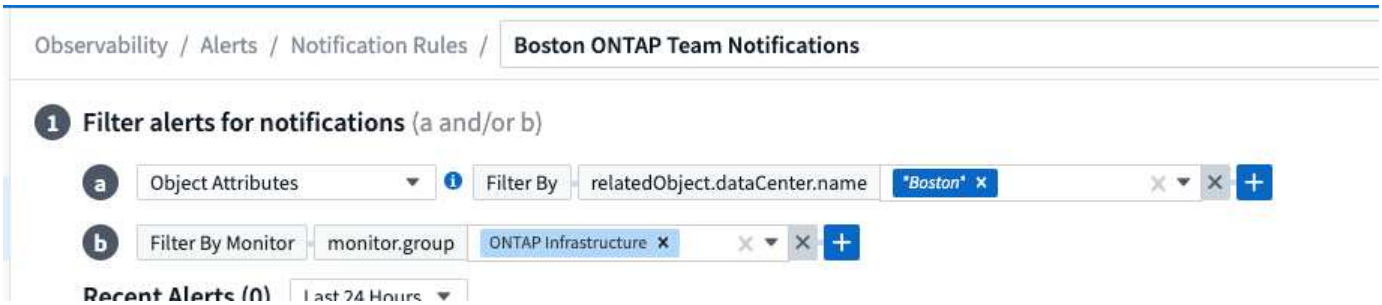
Si noti che vengono soppresse solo le notifiche di avviso (e-mail, webhook); gli avvisi stessi vengono comunque visualizzati nella pagina Osservabilità > Avvisi > Tutti gli avvisi.



Semplifica la gestione degli avvisi con le nuove regole di notifica degli avvisi

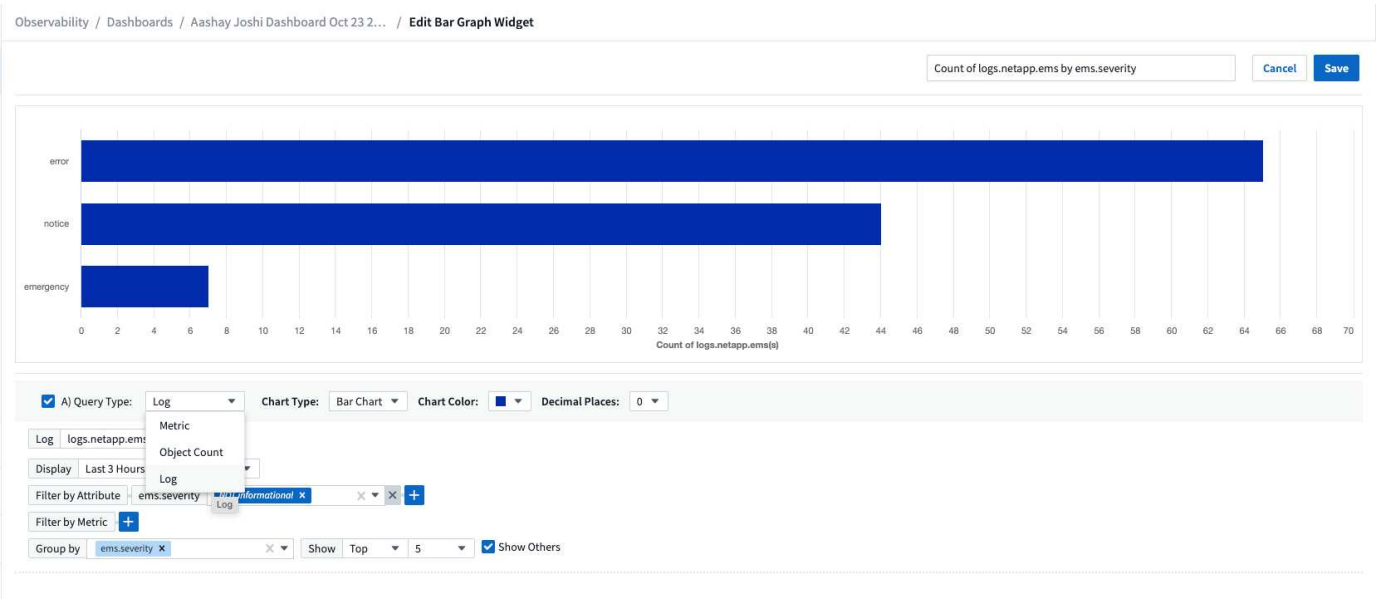
Le regole di notifica degli avvisi semplificano la gestione delle notifiche tra monitor e team.

Controlla la distribuzione degli avvisi sui canali della tua organizzazione, assicurandoti che le informazioni giuste raggiungano il team giusto. Non è necessario gestire monitor separati per team diversi; instradare gli avvisi in base agli attributi degli oggetti correlati (nome dell'archiviazione, data center, nome dell'applicazione) o agli attributi del monitor (gruppo, gravità).



Analisi dei log nelle dashboard

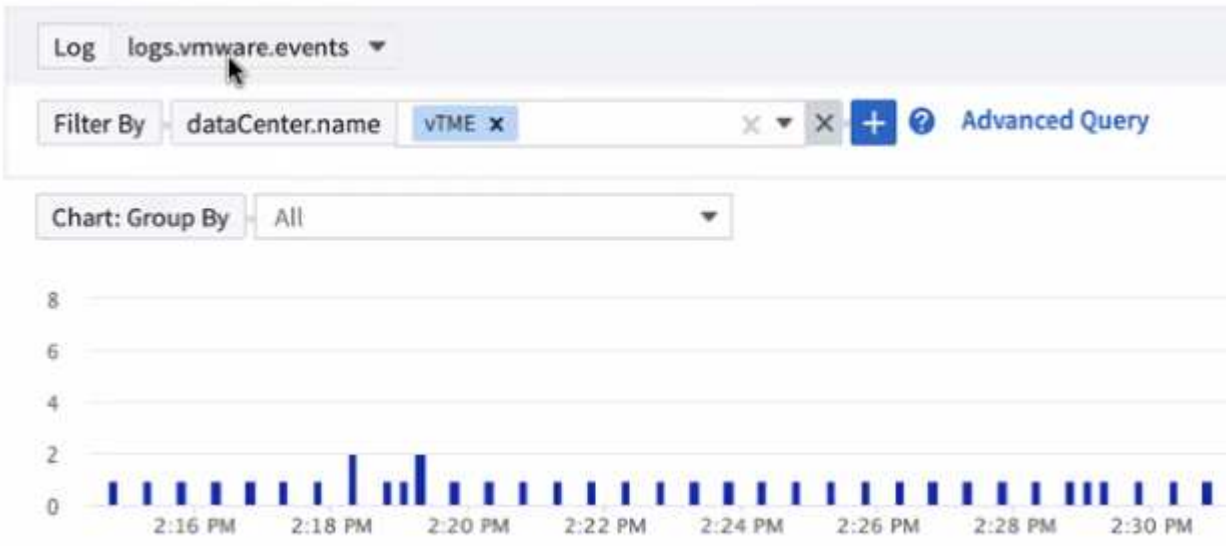
Ora puoi includere gli eventi di registro nelle tue dashboard, per visualizzare i dati degli eventi e avere una comprensione più completa e contestualizzata del tuo ambiente. Esamina i registri e visualizza le metriche correlate senza uscire dalla dashboard!



Migliore osservabilità VMware con VMware Events

Gestisci e risolvi in modo proattivo i problemi del tuo ambiente VMware con eventi in tempo reale. Gli eventi VMware forniscono informazioni dettagliate sulle migrazioni delle VM, sulle allocazioni delle risorse e sullo stato dell'host. Ora disponibile per l'uso in query, dashboard e monitor. Richiede VMware versione 8 o successiva. Selezionare semplicemente la sorgente *logs.vmware.events*.

Gli eventi VMware vengono utilizzati anche per la nuova analisi delle modifiche di configurazione di DII sopra menzionata.



Aggiornamenti del Data Collector:

- **Pure FlashBlade**: questo raccoglitore raccoglie dati di inventario e prestazioni dai cluster FlashBlade che espongono la versione 2 della loro API REST.

Settembre 2024

Presentazione di Data Infrastructure Insights, precedentemente Cloud Insights

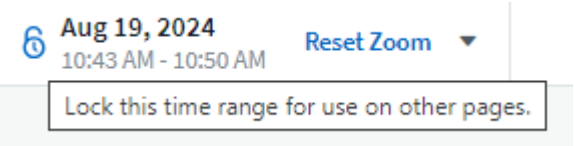
Martedì 24 settembre 2024, NetApp ha ufficialmente cambiato il nome di Cloud Insights in * Data Infrastructure Insights* (DII). Lo ha annunciato Haiyan Song durante la conferenza degli utenti di Insight nel suo discorso principale sul palco principale e in un comunicato stampa sul prodotto della conferenza Insight.

Il servizio DII rimane lo stesso, non ci sono cambiamenti o modifiche nelle funzionalità. Si tratta di un cambio di nome per allineare meglio il nome del servizio alle sue capacità per tutta l'infrastruttura IT.

Agosto 2024

Visualizza i dati specifici per il tuo intervallo di tempo

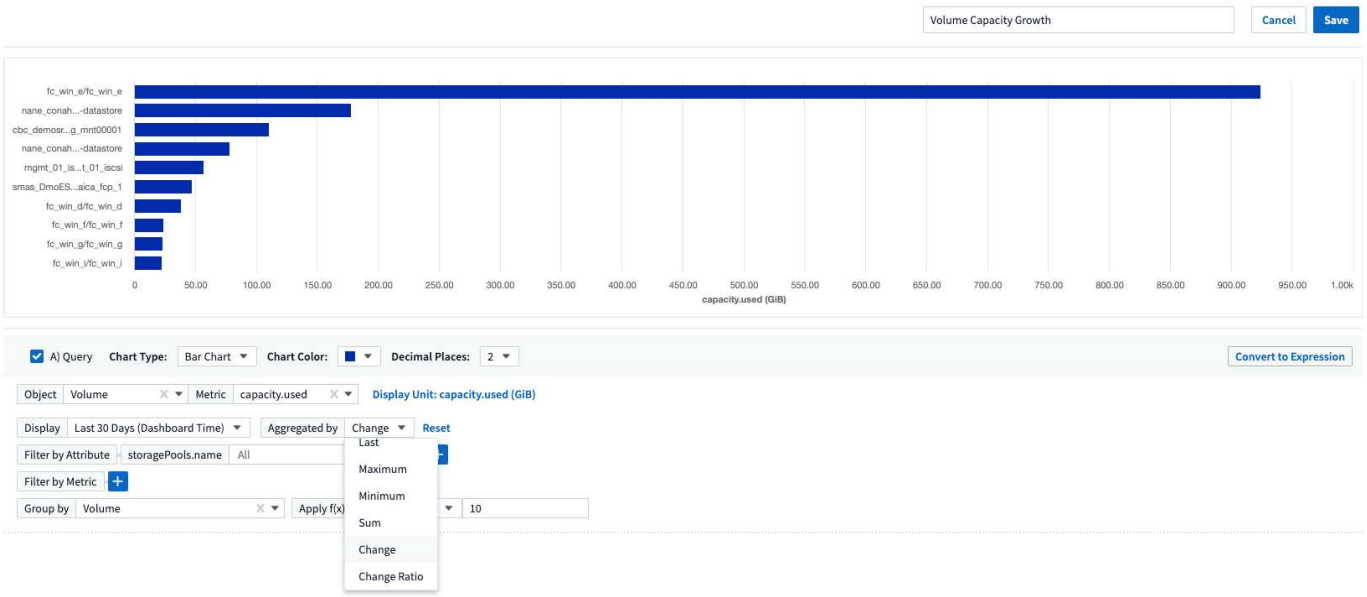
Stai indagando su un avviso? Hai ingrandito un grafico? Queste azioni modificano l'intervallo di tempo per quelle pagine. Ora puoi bloccare quell'intervallo di tempo, passare ad altre pagine Cloud Insights e visualizzare i dati specifici di quell'intervallo di tempo bloccato. Indagare e risolvere i problemi è diventato molto più semplice!



Analisi del cambiamento e del rapporto di cambiamento (%)

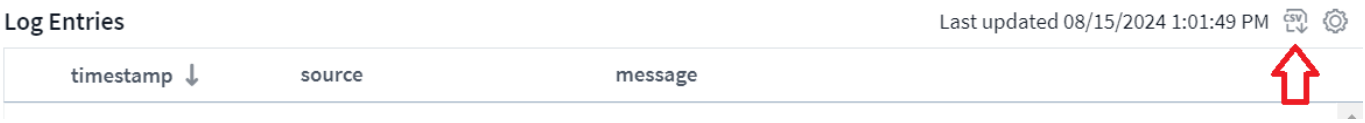
Le aggregazioni temporali del rapporto di variazione aiutano a identificare cambiamenti e tendenze significativi nei valori delle metriche nel tempo. Queste informazioni sono fondamentali per comprendere cosa è cambiato, ad esempio una crescita considerevole della capacità in un periodo di tempo specifico o una modifica nelle prestazioni di un singolo porto.

- **Cambia**: osserva la variazione di una metrica tra due punti all'interno di un periodo selezionato.
- **Rapporto di variazione**: osserva la variazione proporzionale di una metrica tra due punti, rispetto al punto iniziale, entro un periodo selezionato.



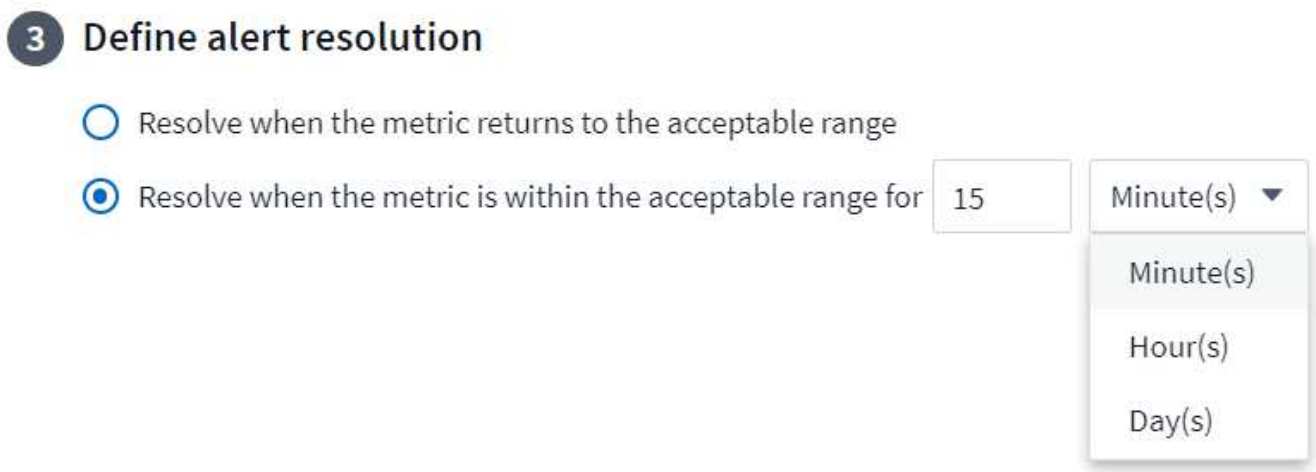
Esporta i risultati delle query del registro in .CSV

Quando visualizzi i risultati delle query di registro, puoi esportare facilmente fino a 10.000 righe in formato .CSV facendo clic sul nuovo pulsante "Esporta". Ciò migliora l'accessibilità dei dati, semplifica l'analisi e la creazione di report sui dati e agevola l'integrazione senza soluzione di continuità con altri strumenti di elaborazione dati.



Risolvi gli avvisi in base al tempo

Cloud Insights ora offre la possibilità di risolvere un avviso quando la metrica monitorata rimane entro l'intervallo accettabile per un periodo di tempo specificato. Ciò consente di concentrarsi sui problemi reali, riducendo il rumore associato alle metriche che superano ripetutamente le soglie definite, consolidando più avvisi in uno.



Luglio 2024

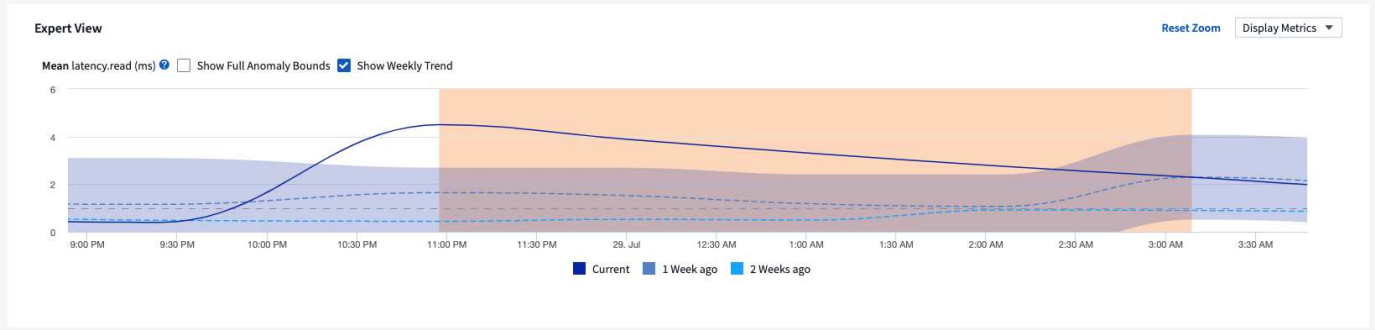
AIOps: rilevamento delle anomalie

Cloud Insights sfrutta l'apprendimento automatico per rilevare cambiamenti imprevisti nei modelli di dati nel tuo ambiente e fornire avvisi proattivi per aiutarti a identificare tempestivamente i problemi.

Un data center si comporta in modo diverso a seconda dell'ora del giorno e del giorno della settimana. Cloud Insights utilizza la stagionalità settimanale per confrontare il comportamento storico per ogni giorno e ora.

Il monitoraggio del rilevamento delle anomalie può fornire avvisi in situazioni in cui la definizione di "normale" non è chiara, in cui il comportamento cambia nel tempo o quando si lavora con grandi quantità di dati in cui la definizione manuale delle soglie non è praticabile.

Nuovo"Monitor di rilevamento delle anomalie" avvisa quando si verificano anomalie come questa sulle metriche degli oggetti da te scelte.



Miglioramenti della sicurezza del carico di lavoro

Supporto NFS 4.1

SVM Data Collector ora supporta le versioni NFS fino a **NFS 4.1** inclusa con ONTAP 9.15.1 o versioni successive.

Nuova API per le attività forensi

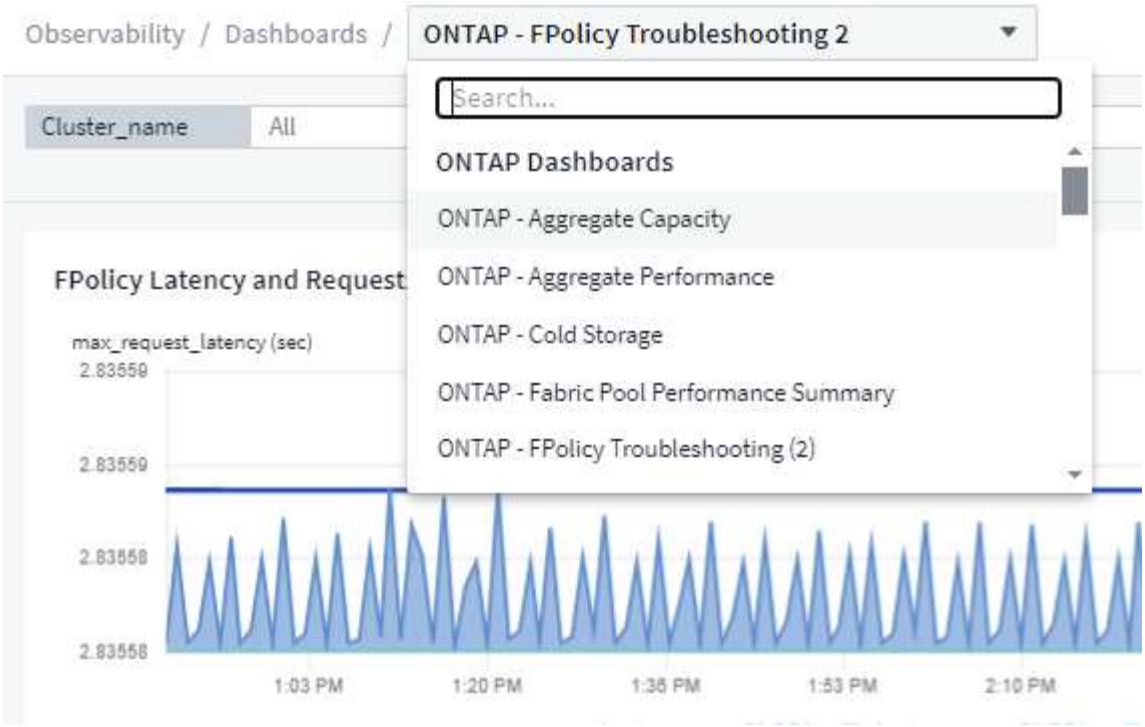
L'attività forense"API" ha una nuova versione. Quando si richiama l'API per Forensics Activity, utilizzare l'API **cloudsecure_forensics.activities.*v2***.

Tieni presente che se effettui più chiamate a questa API, per ottenere risultati ottimali assicurati che le chiamate avvengano in sequenza, anziché in parallelo. Più chiamate parallele potrebbero causare il timeout dell'API.

Navigazione più semplice nella dashboard

Questa funzionalità mira a semplificare i flussi di lavoro operativi e a facilitare la collaborazione tra i team.

Raggruppando le dashboard è più facile ottenere rapidamente la visibilità di cui hai bisogno e ora, con il nuovo menu di navigazione, puoi passare da una dashboard all'altra senza perdere il segno, semplificando l'esplorazione e la gestione della tua infrastruttura. Allinea i gruppi di dashboard con i tuoi runbook operativi per migliorare ulteriormente la tua esperienza.



Giugno 2024

Supporto del sistema operativo

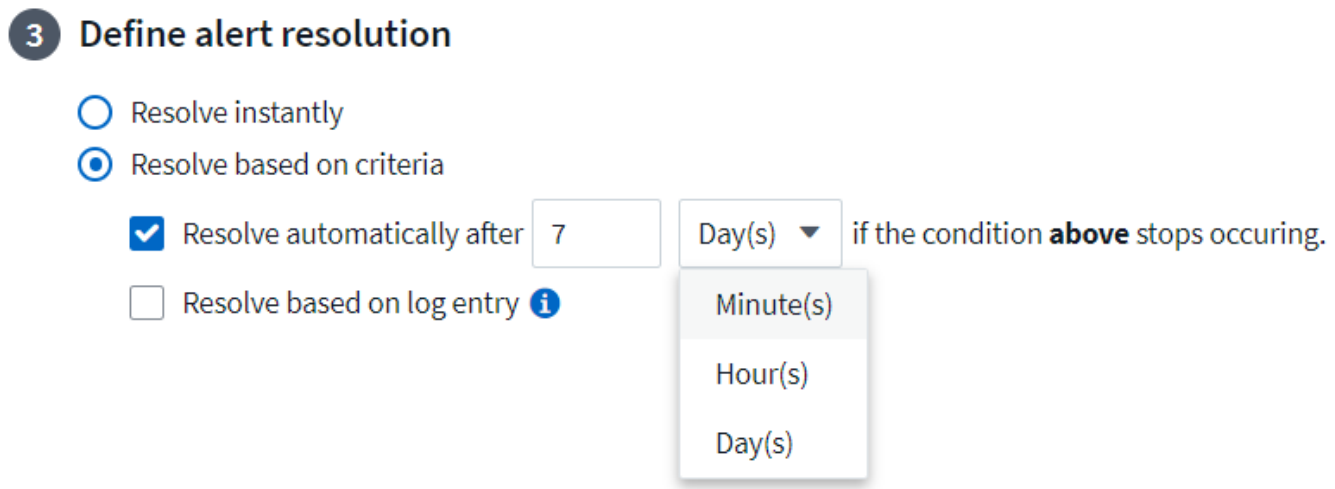
Oltre a quelli supportati da Cloud Insights Acquisition Units, sono supportati anche i seguenti sistemi operativi:"già supportato" :

- Red Hat Enterprise Linux 8.9, 8.10, 9.4
- Rocky 9.4
- AlmaLinux 9.3 e 9.4

Maggio 2024

Risolvi automaticamente gli avvisi in base al tempo

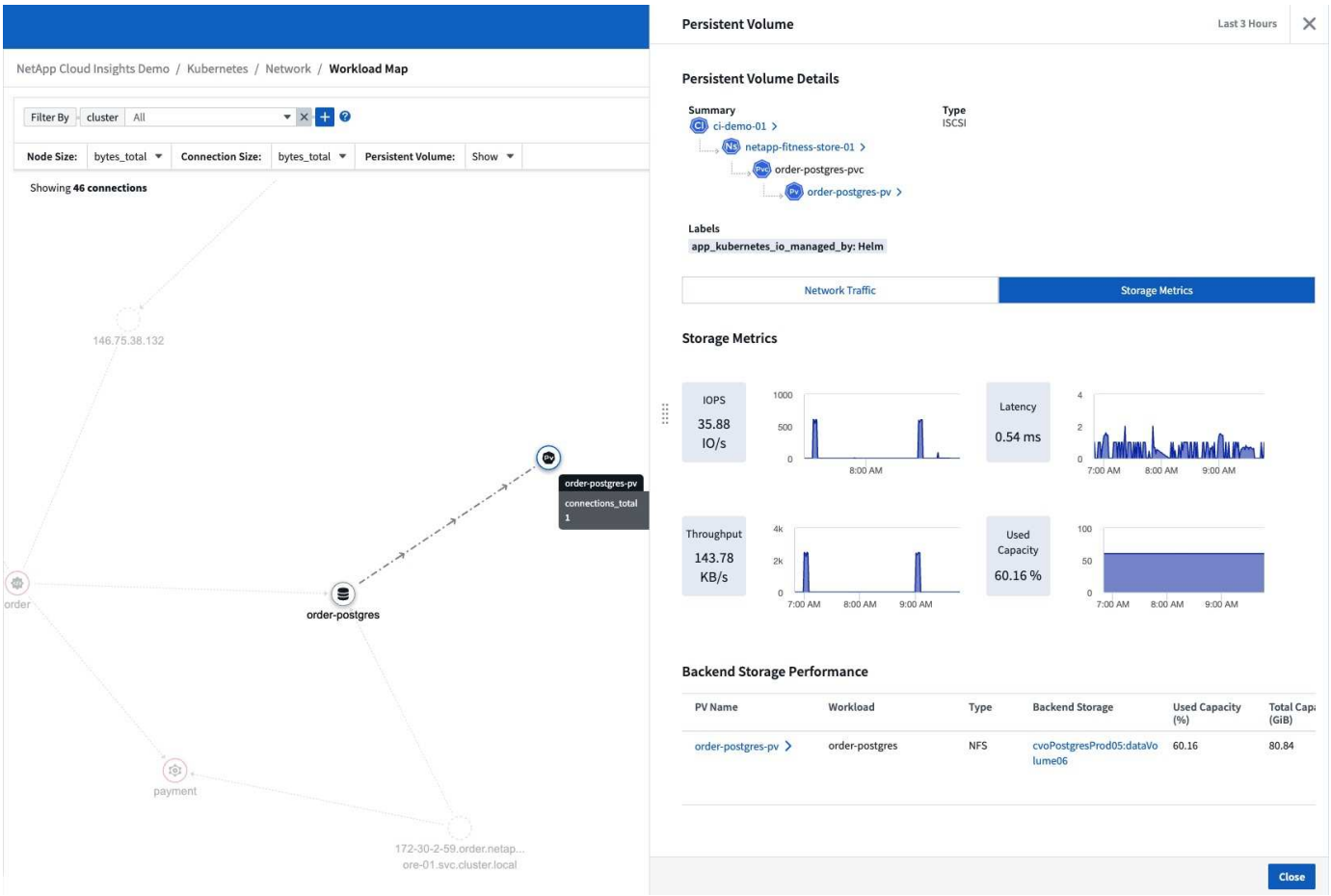
Gli avvisi di registro possono ora essere risolti in base al tempo; se la condizione di avviso cessa di verificarsi, Cloud Insights può risolvere l'avviso automaticamente dopo che è trascorso un periodo di tempo specificato. Puoi scegliere di risolvere l'avviso in minuti, ore o giorni.



Aprile 2024

Supporto iSCSI per Kubernetes

Cloud Insights ora supporta la mappatura dello storage iSCSI associato a Kubernetes, consentendo una risoluzione dei problemi più rapida tramite la mappa di rete Kubernetes e la possibilità di fornire report di chargeback o showback tramite Reporting.



Supporto del sistema operativo

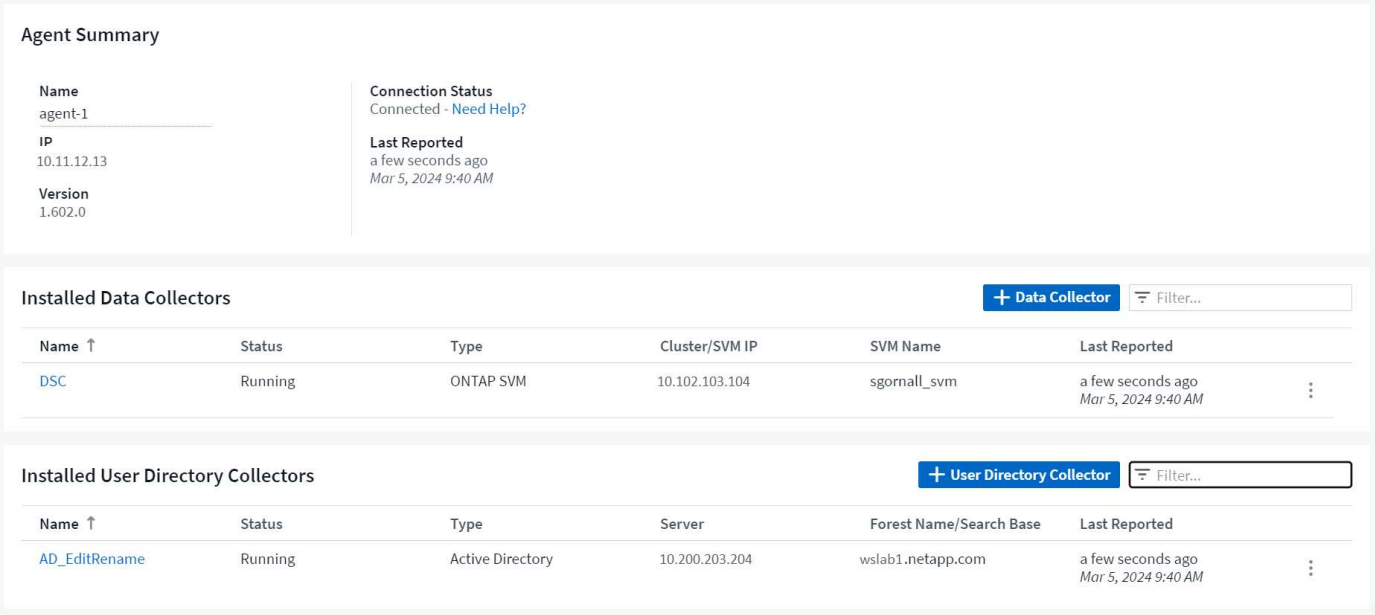
Oltre a quelli supportati da Cloud Insights Acquisition Units, sono supportati anche i seguenti sistemi operativi:"già supportato" :

- Oracle Enterprise Linux 8.8
- Red Hat Enterprise Linux 8.8
- Rocky 9.3
- OpenSUSE Leap dalla 15.1 alla 15.5
- SUSE Enterprise Linux Server 15, 15 SP2 fino a 15 SP5

Marzo 2024

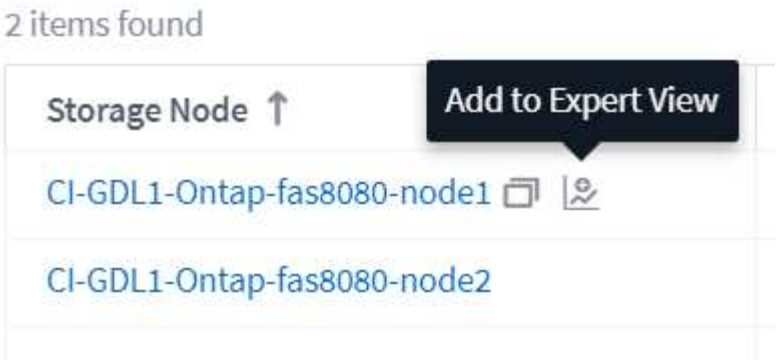
Dettagli dell'agente di sicurezza del carico di lavoro

Ciascuno dei tuoi Workload Security Agent ha la propria landing page, dove puoi facilmente visualizzare informazioni riepilogative sull'agente, nonché sui Data Collector e User Directory Collector installati associati a tale agente.

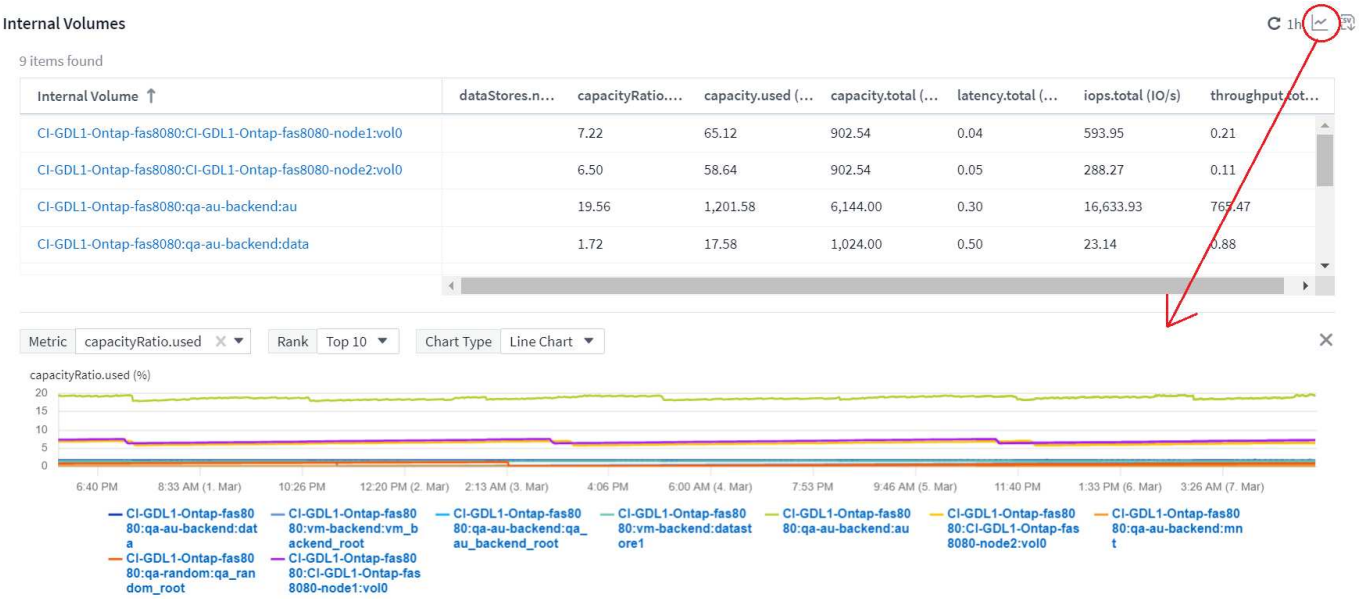


Rappresenta più dati più rapidamente

Quando si analizzano i dati sulla landing page di una risorsa, aggiungere dati aggiuntivi ai grafici di Expert View è un gioco da ragazzi. Per ogni tabella nella landing page, se un tipo di oggetto contiene dati rilevanti, passa il mouse sopra quell'oggetto per visualizzare l'icona "Aggiungi alla vista esperta". Selezionando questa icona l'oggetto verrà aggiunto alle Risorse aggiuntive e visualizzato nei grafici della Vista esperto.



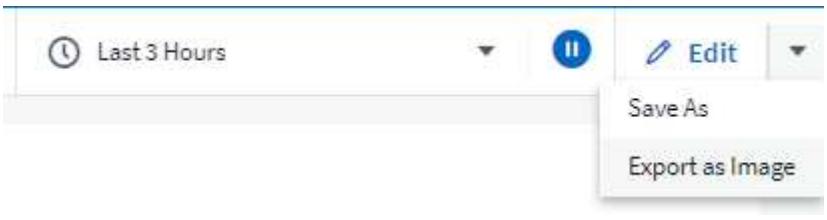
Oppure potresti voler visualizzare i dati di una tabella di landing page in un grafico separato. Basta selezionare l'icona *Mostra grafico* per aprire il grafico sotto la tabella:



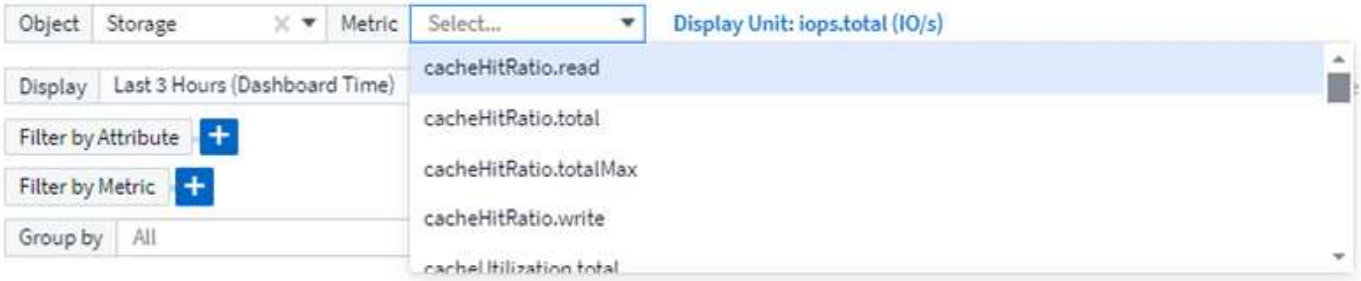
Febbraio 2024

Miglioramenti dell'usabilità

Salva un'istantanea della tua dashboard attuale selezionando *Esporta come immagine* dal menu a discesa nell'angolo destro. Cloud Insights crea un file .PNG degli stati correnti dei widget.

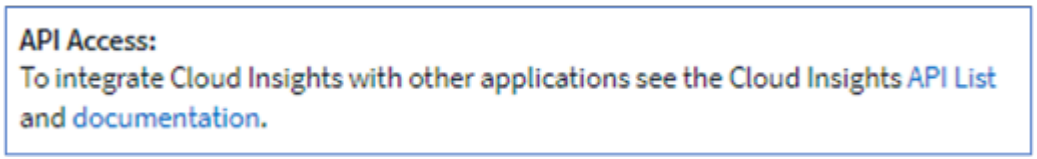


La selezione di oggetti e metriche è più semplice che mai per widget, monitor, ecc. Scegli il tipo di oggetto desiderato, quindi seleziona una metrica pertinente a quell'oggetto nel menu a discesa separato.

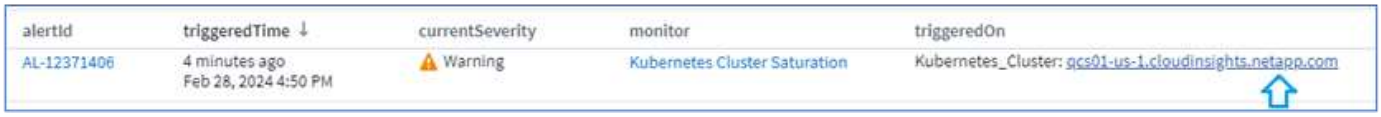


Esporta gli elenchi di Data Collector e Acquisition Unit in formato .CSV selezionando l'icona nella parte superiore di tali pagine.

Abbiamo **riorganizzato la pagina Aiuto > Supporto** in modo che sia più facile trovare ciò che stai cercando e, poiché li hai richiesti, abbiamo aggiunto in questa pagina dei link diretti ad **API Swagger** e alla documentazione utente.

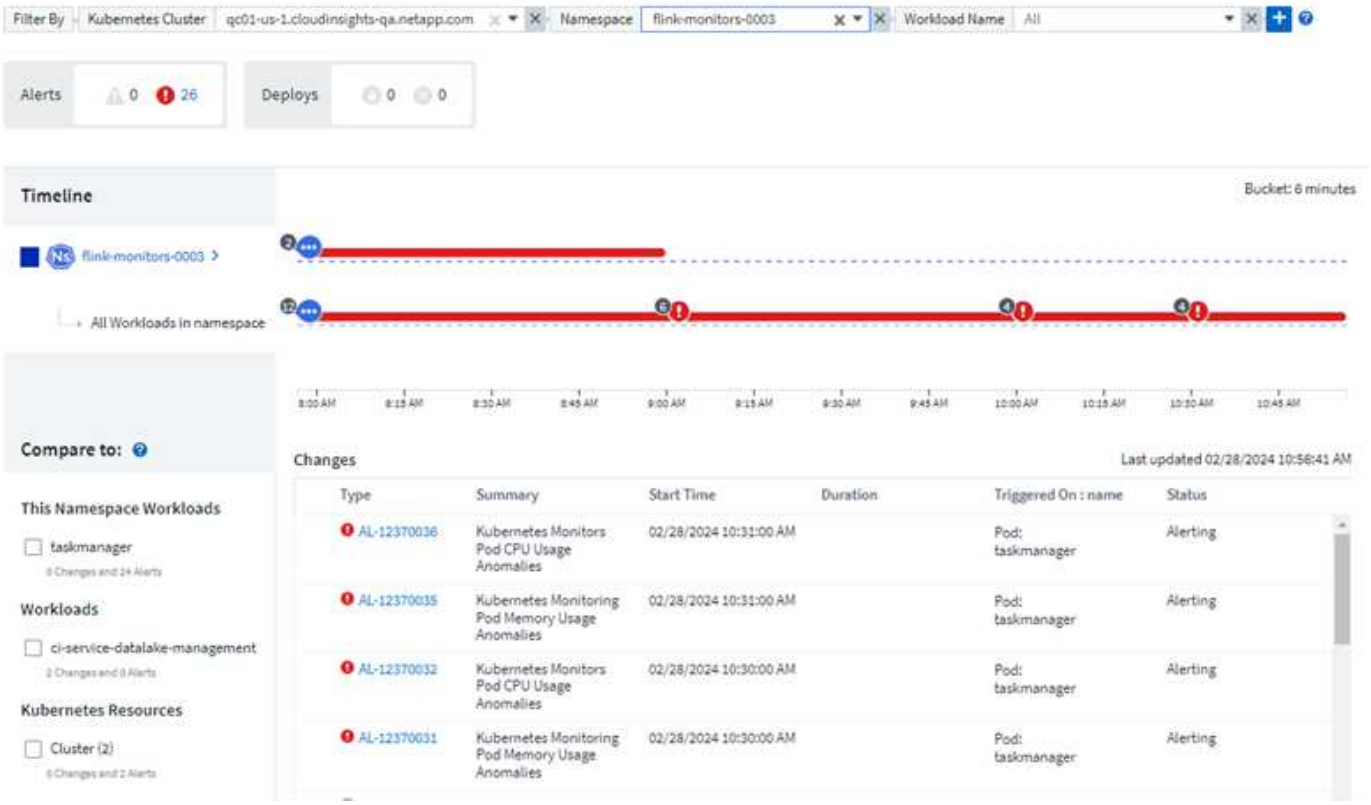


I link nella colonna "triggeredOn" nella pagina dell'elenco degli avvisi condurranno alla landing page appropriata, se è disponibile una landing page per quell'oggetto.



Visualizza tutte le modifiche nel tuo namespace

Kubernetes Change Analysis ora consente di visualizzare una cronologia delle modifiche quando si seleziona Cluster e Namespace. In precedenza, era necessario selezionare anche Carico di lavoro. Quando si filtra per Cluster e Namespace, la cronologia di tutte le modifiche del carico di lavoro in quello namespace viene visualizzata su una riga.



Registri correlati per gli avvisi

Quando si visualizza un avviso di registro, le voci di registro correlate vengono mostrate in una nuova tabella. Una voce di registro è correlata se si verifica nella stessa origine e nello stesso intervallo di tempo dell'avviso ed è soggetta alle stesse condizioni. Seleziona "Analizza registri" per approfondire.

Raccogliere i dati dello switch ONTAP

Cloud Insights può raccogliere dati dagli switch back-end del sistema ONTAP ; è sufficiente abilitare la raccolta nella sezione *Configurazione avanzata* del raccoglitore dati e assicurarsi che il sistema ONTAP sia configurato per fornire"informazioni sullo switch" e ha l'appropriato"permessi" impostato.

API del raccoglitore dati per la sicurezza del carico di lavoro

Negli ambienti di grandi dimensioni, è possibile automatizzare la creazione del collettore Workload Security utilizzando la nuova API Data Collectors. Per saperne di più, vai su **Amministrazione > Accesso API > Documentazione API** e seleziona il tipo di API *Sicurezza del carico di lavoro*.

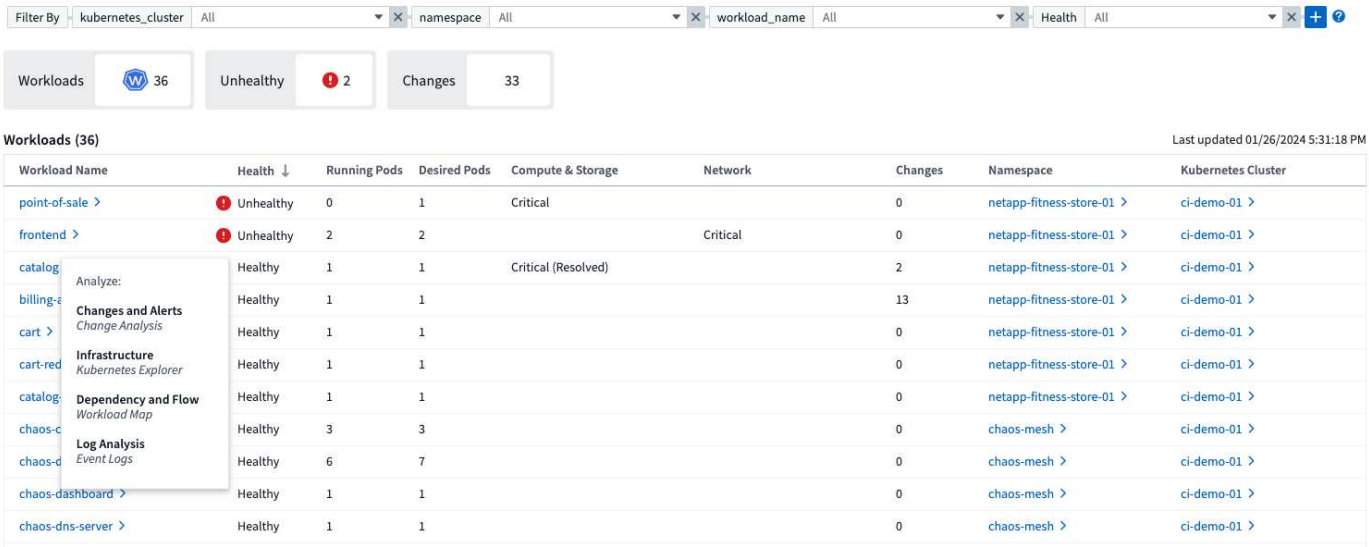
Gennaio 2024

Prova le funzionalità di Cloud Insights che non hai ancora utilizzato

Oltre alla prova iniziale di Cloud Insights, puoi anche usufruire di"Valutazioni dei moduli" . Ad esempio, se sei abbonato a Cloud Insights e hai monitorato l'archiviazione e le macchine virtuali, quando aggiungi Kubernetes al tuo ambiente, entrerai automaticamente in una prova di 30 giorni di Kubernetes Observability. L'utilizzo delle unità gestite da Kubernetes Observability non verrà conteggiato nel diritto sottoscritto fino al termine del periodo di prova.

Quanto sono sani i miei carichi di lavoro?

Lo stato del carico di lavoro è disponibile a colpo d'occhio nella pagina **Kubernetes > Esplora > Carichi di lavoro**, così puoi vedere rapidamente quali carichi di lavoro funzionano bene e quali potrebbero aver bisogno di aiuto. Identifica facilmente se il problema di salute è correlato a modifiche dell'infrastruttura, della rete o della configurazione e analizza in dettaglio la causa principale.



Aggiornamenti del Data Collector

Identificazione del dominio dei dati

Il raccoglitore Data Domain è stato migliorato per identificare meglio i sistemi HA per la durabilità durante gli eventi di failover. Questa modifica causerà una reidentificazione **una tantum** degli appliance Data Domain nei sistemi HA, che successivamente causerà la rimozione di tutte le annotazioni su tali risorse (perché questi array verranno reidentificati). Sarà necessario ricollegare le annotazioni agli oggetti Data Domain.

Algoritmo ML avanzato per il rilevamento del ransomware

Workload Security include un nuovo algoritmo ML di rilevamento ransomware di seconda generazione per rilevare gli attacchi più sofisticati in modo più rapido e accurato.

"Stagionalità" dei comportamenti: il comportamento del fine settimana può seguire schemi diversi da quello dei giorni feriali, o il comportamento mattutino da quello pomeridiano. Gli algoritmi di sicurezza del carico di lavoro tengono conto di questa stagionalità.

Funzionalità deprecate

Occasionalmente, man mano che le funzionalità si evolvono, alcune funzionalità vengono deprecate. Ecco alcune delle funzionalità e caratteristiche che sono state deprecate in Cloud Insights:

L'API Workload Secure REST cloudsecure_forensics.activities.v1 è obsoleta

L'API *cloudsecure_forensics.activities.v1* è obsoleta. Questa API restituisce informazioni sulle attività associate alle entità nell'ambiente Storage Workload Security. Questa API è stata sostituita con cloudsecure_forensics.activities.*v2*_.

In precedenza, GET per questa API restituiva quanto segue:

```
{
  "count": 24594,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "accessLocation":
```

Questa API ora restituisce:

```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lvlvk3pp.4cpzcg4kpybl",
      "before": "lvlxy3dz.4cq5ajdnl9fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

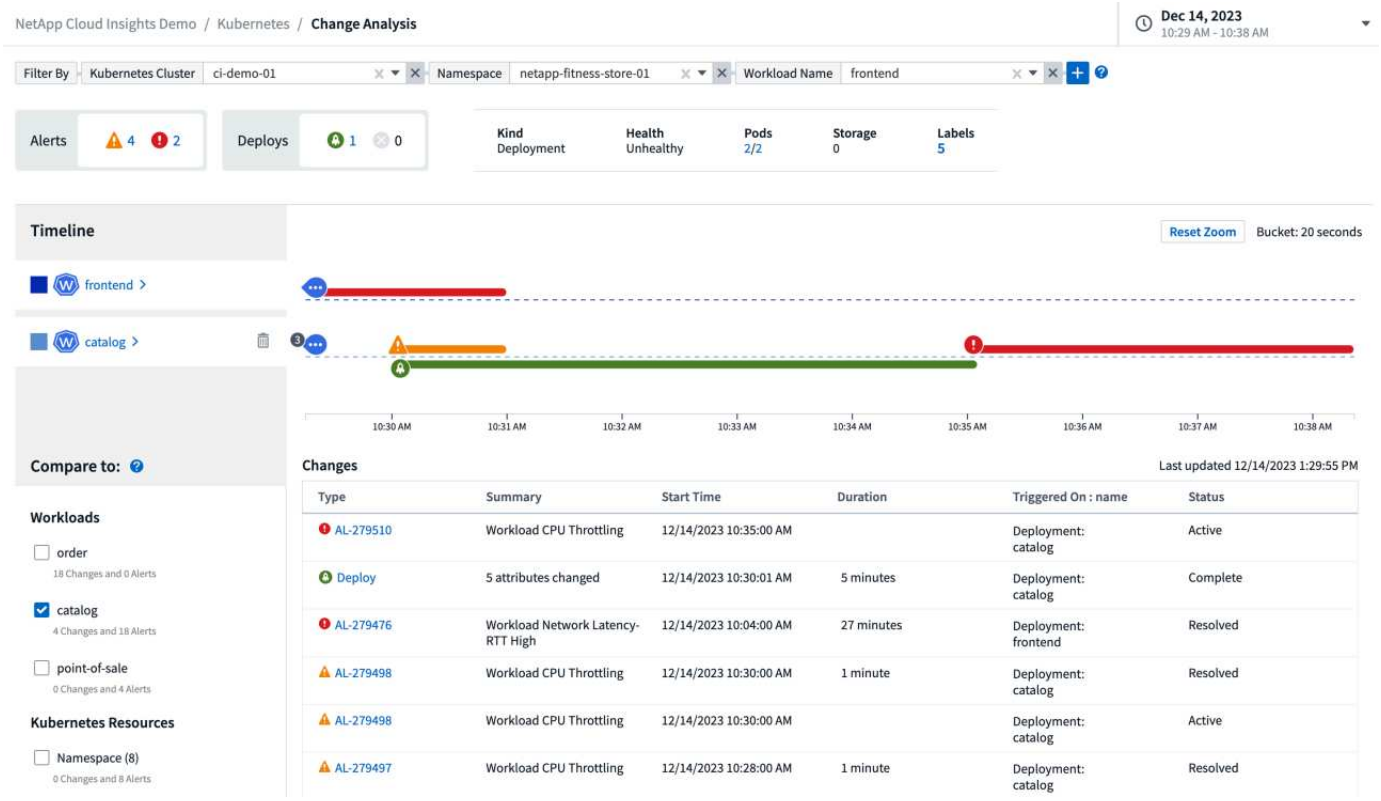
Per maggiori dettagli, consultare la documentazione di Swagger in **Amministrazione › Accesso API › Documentazione API › Sicurezza del carico di lavoro**.

Dicembre 2023

Analisi dei cambiamenti in sintesi

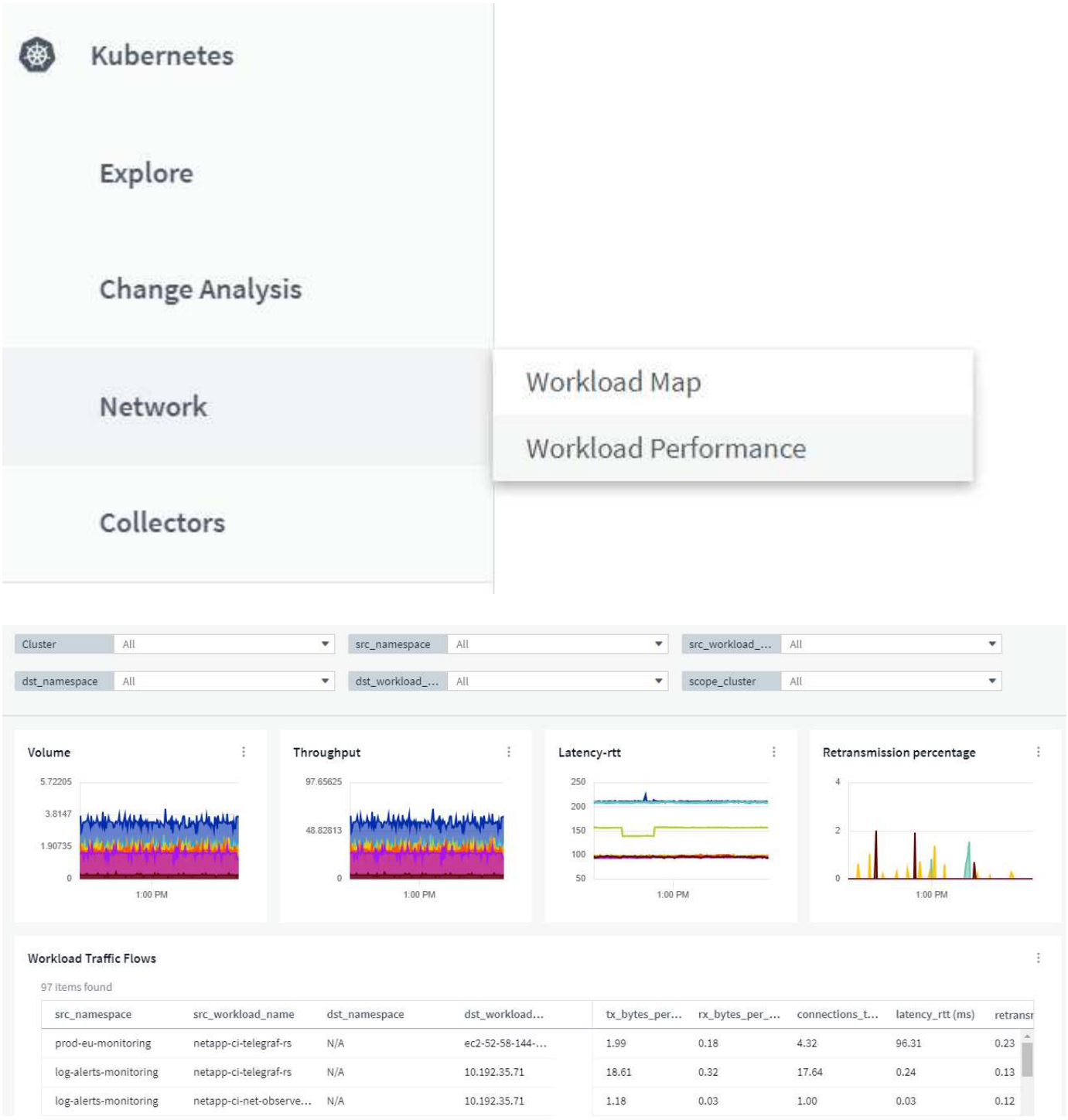
Kubernetes"Analisi dei cambiamenti" fornirti una visione completa delle modifiche recenti apportate al tuo ambiente Kubernetes. Avvisi e stato di distribuzione sono a portata di mano. Con Change Analytics puoi

monitorare ogni modifica di distribuzione e configurazione e correlarla allo stato di salute e alle prestazioni dei servizi, dell'infrastruttura e dei cluster di K8.



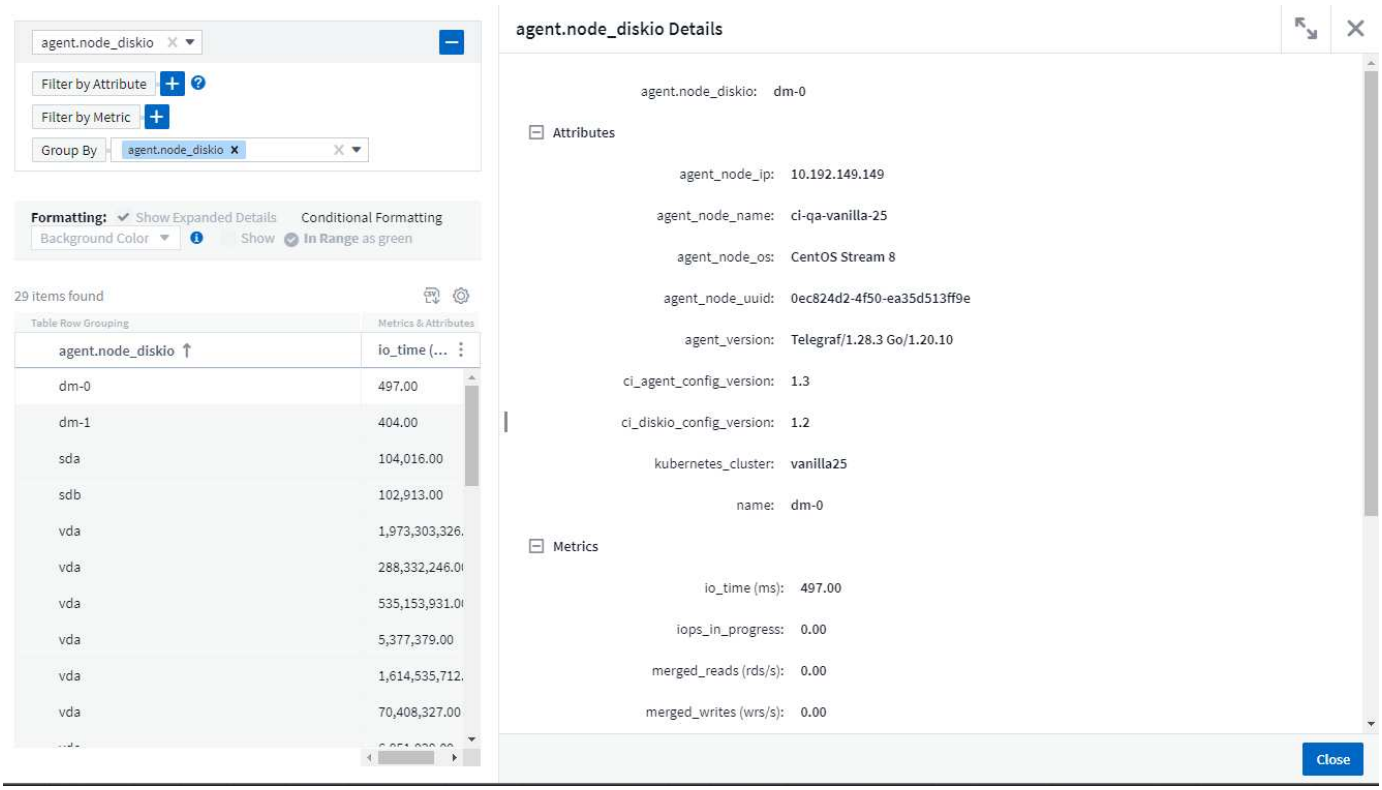
Dashboard delle prestazioni del carico di lavoro di Kubernetes

Le prestazioni del carico di lavoro sono immediatamente disponibili nella dashboard completa Kubernetes Workload Performance. Visualizza rapidamente grafici delle tendenze di volume, throughput, latenza e ritrasmissione, nonché una tabella del traffico del carico di lavoro per ogni namespace nel tuo ambiente. I filtri consentono di focalizzare facilmente le aree di interesse.



Dettagli della query in una schermata

In una query, selezionando una riga si apre un pannello laterale che mostra i dettagli degli attributi, delle annotazioni e delle metriche per la riga selezionata, fornendo informazioni utili senza dover approfondire la landing page dell'oggetto. I link nella riga o nel pannello laterale consentono una facile navigazione.



Aggiornamenti del Data Collector:

- * Brocade FOS REST*: questo raccoglitore è stato rimosso da "Anteprima" ed è ora generalmente disponibile. Alcune cose da notare:
  - FOS ha introdotto la sua API REST con FOS 8.2. Tuttavia, alcune funzionalità, come il routing, hanno ricevuto le funzionalità REST API solo con la versione 9.0.
  - Se si dispone di un fabric composto da asset FOS misti con versione 8.2 superiore e alcuni con versione < 8.2, il raccoglitore REST FOS Cloud Insights non riuscirà a rilevare tali asset meno recenti. È possibile modificare il collettore REST FOS e creare un elenco delimitato da virgole degli indirizzi IPv4 di tali dispositivi da escludere da tale collettore.
- **SELinux**: Cloud Insights include miglioramenti all'installazione iniziale di Linux Acquisition Unit per garantire la robustezza del funzionamento negli ambienti Linux con l'applicazione SELinux abilitata. Questi miglioramenti hanno effetto solo sulle *nuove* distribuzioni AU; se riscontri problemi con SELinux relativi agli aggiornamenti AU, contatta l'assistenza NetApp per correggere la configurazione SELinux.

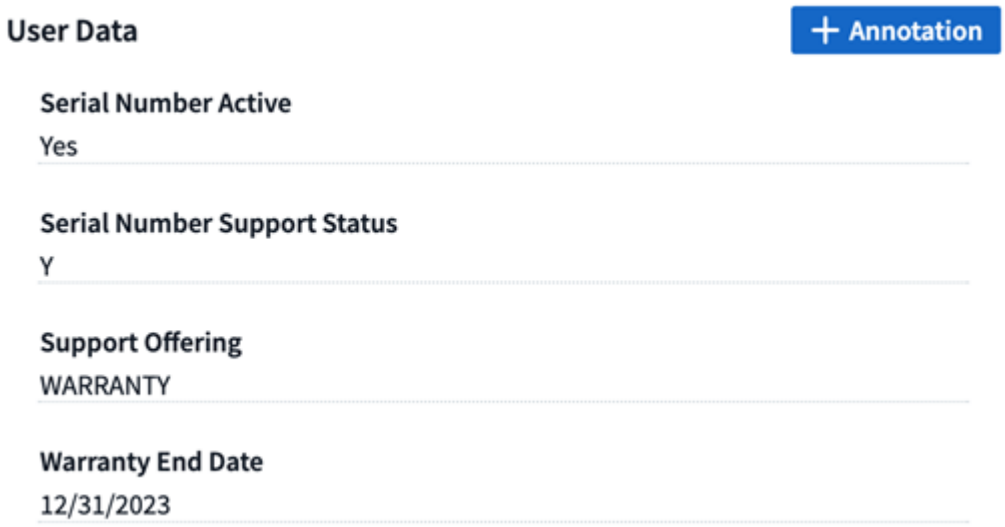
Novembre 2023

Sicurezza del carico di lavoro: sospendi/riprendi un collettore

In Workload Security, è possibile mettere in pausa un Data Collector se il collector è in stato *In esecuzione*. Aprire il menu "tre punti" del raccoglitore e selezionare PAUSA. Mentre il collettore è in pausa, nessun dato viene raccolto da ONTAP e nessun dato viene inviato dal collettore a ONTAP. Seleziona Riprendi per ricominciare a riscuotere.

Informazioni sul supporto del nodo di archiviazione

Nella landing page di un nodo di archiviazione, la sezione *Dati utente* fornisce informazioni immediate sull'offerta di supporto, sullo stato attuale, sullo stato del supporto e sulla data di fine della garanzia. Tieni presente che attualmente Cloud Insights pubblica automaticamente queste informazioni solo per i dispositivi NetApp . Si noti inoltre che questi campi di supporto sono annotazioni, quindi possono essere utilizzati in query e dashboard.



Mappa i tag VMWare alle annotazioni Cloud Insights

IL"VMware" Il raccoglitore dati consente di popolare le annotazioni di testo Cloud Insights con tag con lo stesso nome configurati su VMWare.

Miglioramenti dell'affidabilità del collettore CLI Brocade per FOS 9.1.1c e firmware superiore

Su alcuni switch Brocade Fibre Channel che eseguono il firmware 9.1.1c, l'output di alcuni comandi CLI potrebbe essere preceduto dal testo del banner di accesso "motd" o da avvisi che invitano gli utenti a modificare le password predefinite. Il raccoglitore Brocade CLI è stato migliorato per ignorare questi due tipi di testo estraneo.

Prima di questo miglioramento, solo gli switch FOS 9.1.1c senza Virtual Fabric erano probabilmente rilevabili con questo tipo di collettore.

Ottobre 2023

Sicurezza avanzata del carico di lavoro

La sicurezza del carico di lavoro è stata migliorata con quanto segue:

- **Accesso negato**: Workload Security si integra con ONTAP per ricevere"Eventi "Accesso negato"" e fornire un ulteriore livello di analisi e risposte automatiche.
- **Tipi di file consentiti**: se viene rilevato un attacco ransomware per un'estensione di file nota, tale

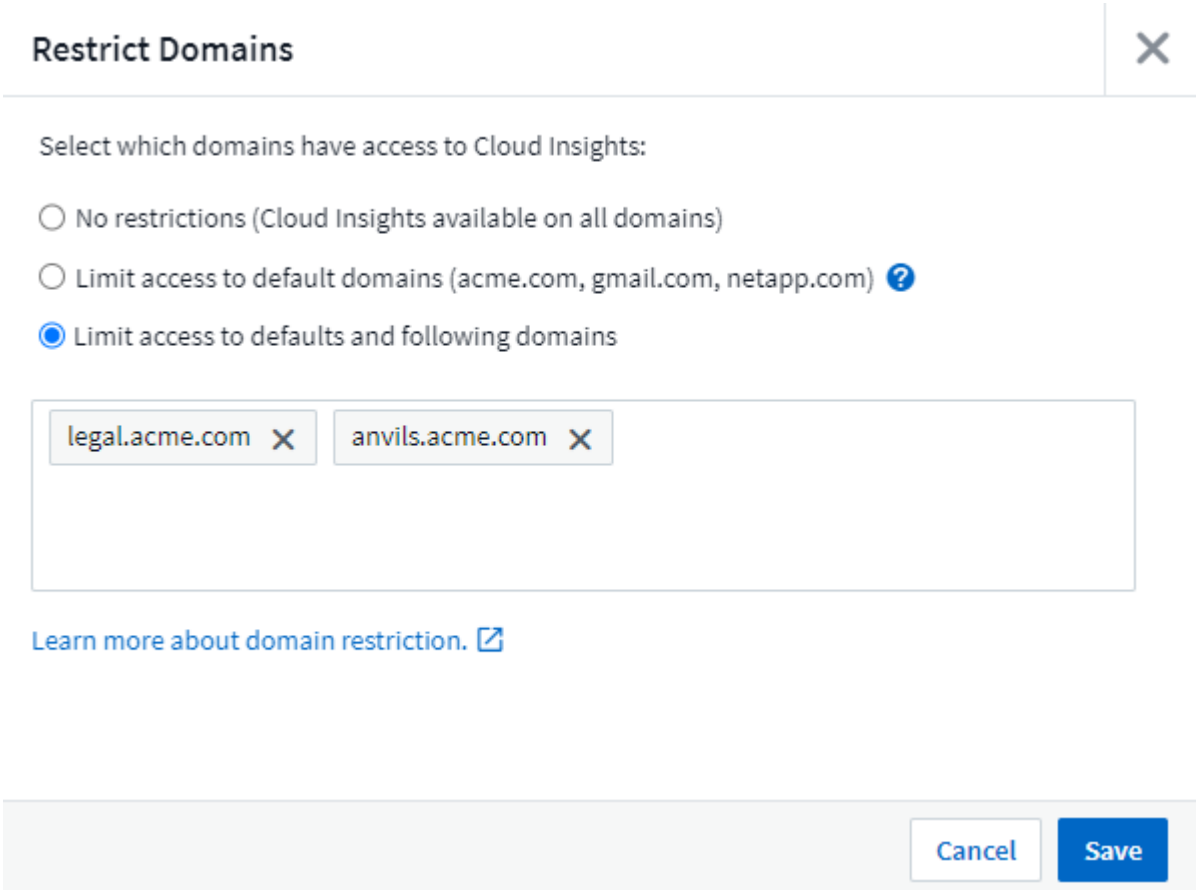
estensione di file può essere aggiunta a un"tipi di file consentiti" elenco per evitare avvisi non necessari.

Prove del modulo

Oltre alla prova iniziale di Cloud Insights, puoi anche usufruire di"Valutazioni dei moduli" . Ad esempio, se sei già abbonato a Infrastructure Observability ma stai aggiungendo Kubernetes al tuo ambiente, entrerai automaticamente in una prova gratuita di 30 giorni di Kubernetes Observability. Al termine del periodo di valutazione ti verrà addebitato solo l'utilizzo dell'unità gestita da Kubernetes Observability.

Limita l'accesso ai domini specificati

Gli amministratori e i proprietari degli account ora hanno la possibilità di"limitare l'accesso a Cloud Insights" per inviare e-mail ai domini da loro specificati. Vai su **Amministrazione > Gestione utenti** e seleziona il pulsante *Limita domini*.



Aggiornamenti del Data Collector

Sono in atto le seguenti modifiche all'unità di raccolta/acquisizione dati:

- **Isilon / PowerScale REST**: sono stati aggiunti vari nuovi attributi e metriche alle funzionalità di analisi avanzate Cloud Insights con il nome *emc_isilon.node_pool.**. Questi contatori e attributi consentiranno agli utenti di creare dashboard e monitor per il consumo di capacità del *node_pool*; gli utenti con cluster Isilon creati da modelli di nodi hardware diversi avranno più pool di nodi e comprendere il consumo di capacità totale/HDD/SSD a livello di pool di nodi è utile sia per il monitoraggio che per la pianificazione.
- **Rubrik** Supporto per l'autenticazione "account di servizio": il raccoglitore Rubrik di Cloud Insights ora supporta sia l'autenticazione di base HTTP tradizionale (nome utente e password) sia l'approccio dell'account di servizio di Rubrik, che richiede un nome utente + segreto + ID organizzazione.

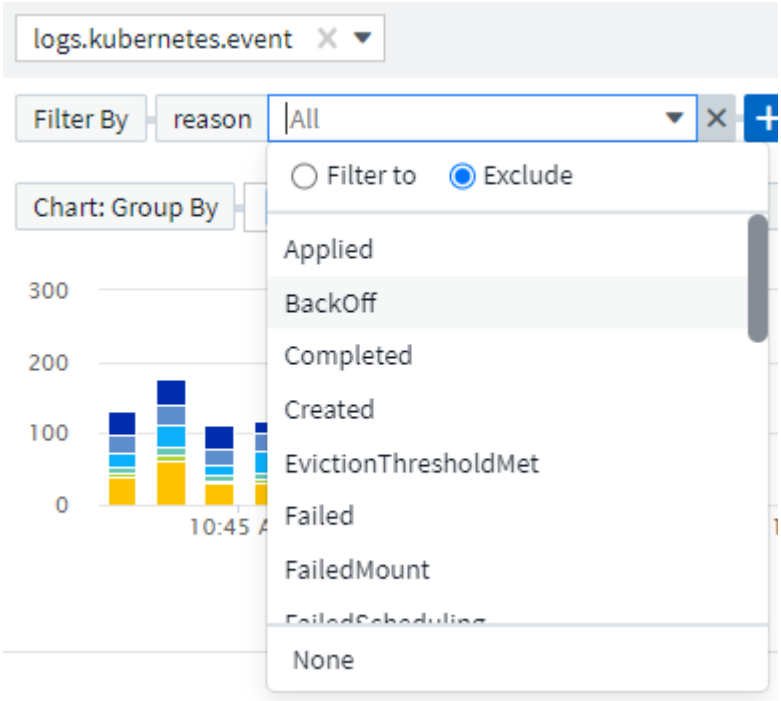
Settembre 2023

Trova facilmente ciò che desideri nei registri

La query di registro (**Osservabilità > Query di registro > +Nuova query di registro**) include una serie di"miglioramenti" per rendere l'esplorazione dei log più semplice e informativa.

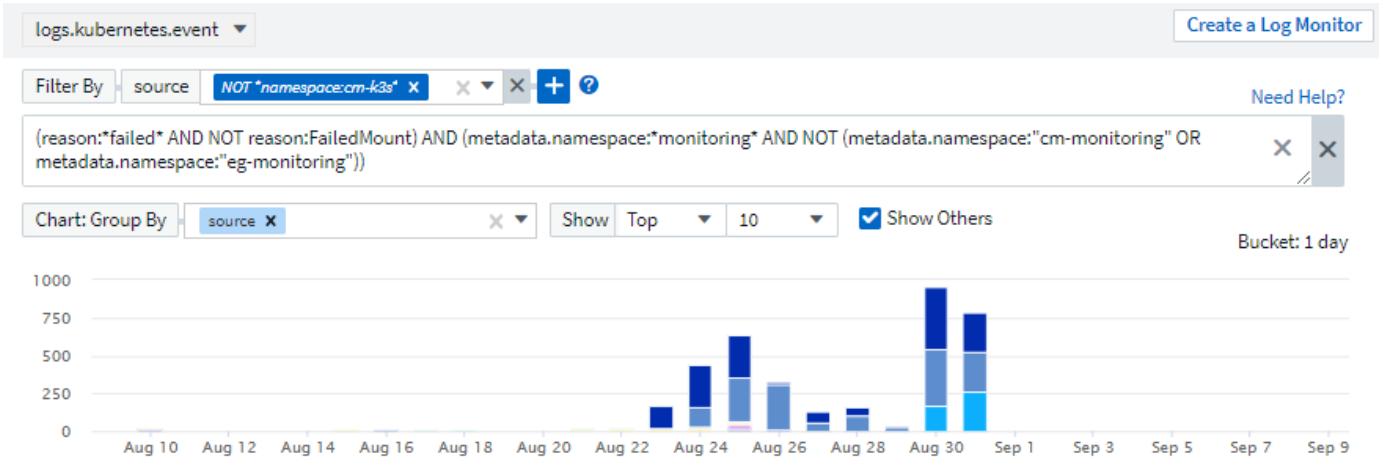
Includi/Escludi

Quando si filtra un valore, è possibile scegliere facilmente se **Includere** o **Escludere** i risultati che corrispondono al filtro. Selezionando "Escludi" viene creato un filtro "NOT <valore>". È possibile combinare i valori Includi ed Escludi in un unico filtro.



Query avanzata

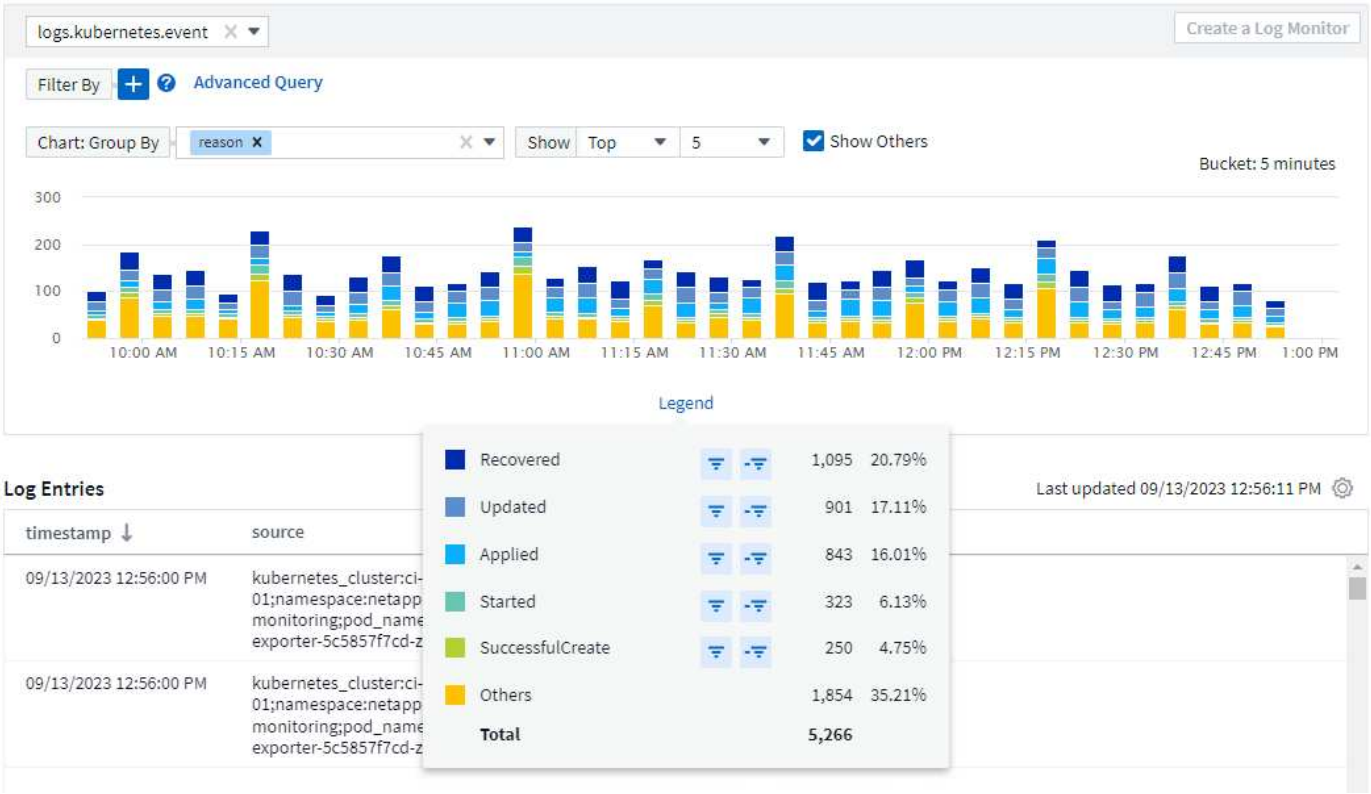
Advanced Querying ti dà la possibilità di creare filtri "in formato libero", combinando o escludendo valori utilizzando AND, NOT, OR, caratteri jolly, ecc.



Le query "Filtra per" e "Avanzata" vengono combinate tramite "AND" per formare un'unica query. I risultati vengono visualizzati nell'elenco dei risultati e nel grafico.

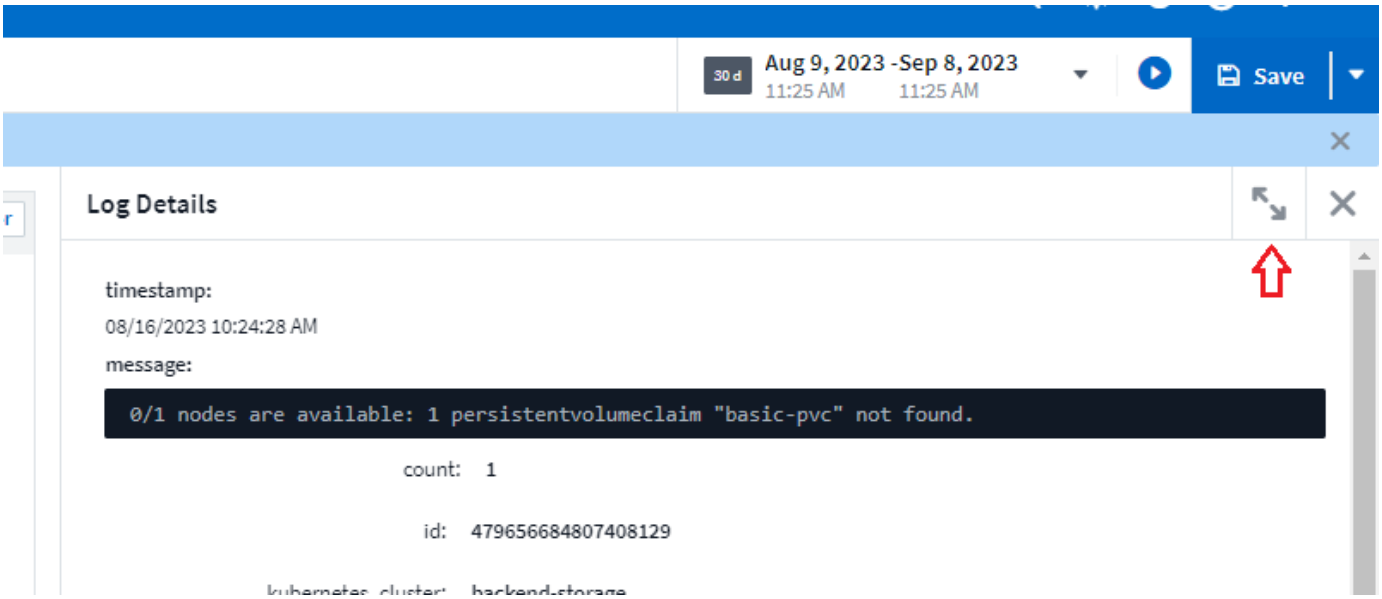
Raggruppamento nel grafico

Quando si seleziona un attributo di registro per **Raggruppare per**, l'elenco e il grafico mostrano i risultati del filtro corrente. Nel grafico, le colonne sono raggruppate in base ai colori. Passando il mouse su una colonna del grafico verranno visualizzati i dettagli sulle voci specifiche, simili alle informazioni generali visualizzate quando si espande la legenda del grafico. Nella legenda puoi anche scegliere di impostare un filtro Includi o Escludi per un raggruppamento specifico.



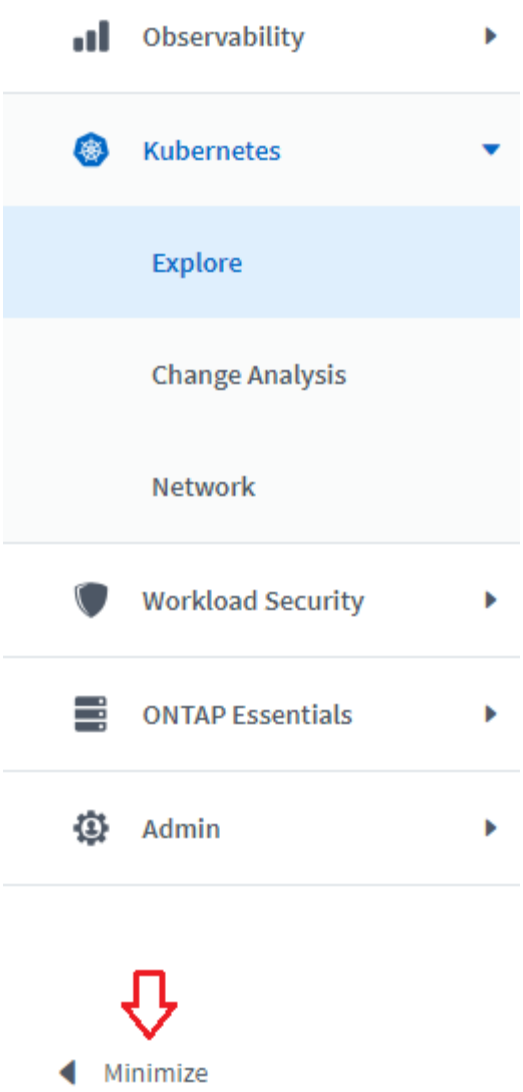
Pannello di dettaglio del registro "fluttuante"

Quando si esplorano i registri utilizzando la query di registro, selezionando una voce nell'elenco si apre un pannello dei dettagli per quella voce. Ora puoi scegliere di visualizzare il pannello scorrevole come "Mobile" (ovvero visualizzato sul resto dello schermo) o "Nella pagina" (ovvero visualizzato come un riquadro a sé stante all'interno della pagina). Per passare da una visualizzazione all'altra, seleziona il pulsante "Nella pagina/Floating" nell'angolo in alto a destra del pannello.



Comprimi il menu

È possibile ridurre a icona il menu di navigazione Cloud Insights sul lato sinistro selezionando il pulsante "Riduci a icona" sotto il menu. Quando il menu è ridotto a icona, passa il mouse su un'icona per vedere quale sezione si apre; selezionando l'icona si apre il menu e si accede direttamente a quella sezione.



Miglioramenti del Data Collector

Cloud Insights ha semplificato la visualizzazione e la ricerca delle informazioni del raccoglitore dati:

- **L'elaborazione degli elenchi dei raccoglitori di dati** è più efficiente, il che significa che il tempo necessario per visualizzare e navigare in questi elenchi è notevolmente ridotto. Se disponi di un ambiente di grandi dimensioni con molti collettori di dati, noterai un miglioramento significativo nell'elencare i tuoi collettori di dati.
- La **Data Collector Support Matrix** è passata da un file .PDF a una pagina basata su .HTML, più rapida da navigare e più facile da gestire. Scopri il nuovo Matrix qui: https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

Agosto 2023

Raccolta di registri Isilon/PowerScale e dati di analisi avanzata

I collettori REST Isilon e REST PowerScale contengono i seguenti miglioramenti:

- Gli eventi del registro Isilon sono disponibili per l'uso in query e avvisi
- Gli attributi di Isilon Advanced Analytic sono disponibili per l'uso in query, dashboard e avvisi:
  - emc_isilon.cluster
  - emc_isilon.node
  - emc_isilon.node_disk
  - emc_isilon.net_iface

Sono abilitati per impostazione predefinita per gli utenti dei collettori Isilon REST e/o PowerScale REST. NetApp consiglia vivamente agli utenti del collector basato su Isilon CLI di migrare al nuovo collector basato su REST API per usufruire di miglioramenti come quelli sopra indicati.

Mappa del carico di lavoro migliorata

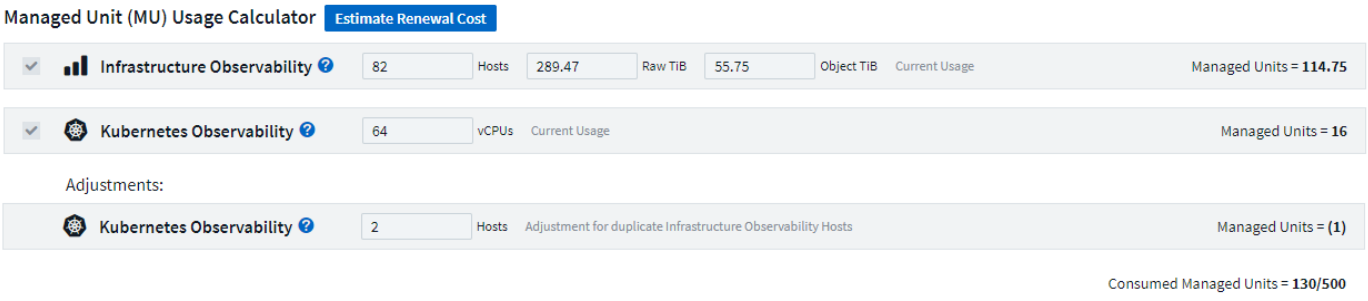
La mappa del carico di lavoro è più utilizzabile e meno rumorosa; raggruppa tutti i servizi esterni simili in un unico nodo se comunicano con gli stessi carichi di lavoro, riducendo la complessità del grafico e rendendo più semplice comprendere come i servizi sono interconnessi.

Scegliendo un nodo raggruppato verrà visualizzata una tabella dettagliata con le metriche del traffico di rete per ciascun servizio esterno pertinente a quel nodo.

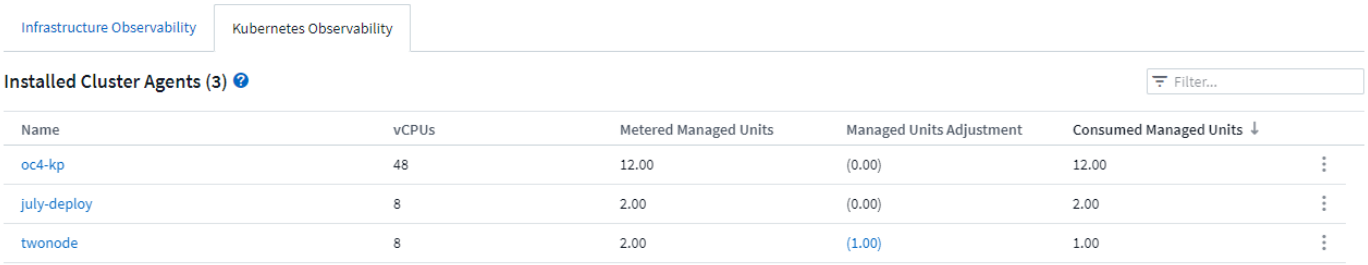
Regolazione dell'utilizzo delle unità gestite di Kubernetes

Nel caso in cui una risorsa di elaborazione nel tuo ambiente cluster Kubernetes venga conteggiata sia da NetApp Kubernetes Monitoring Operator sia da un raccoglitore di dati dell'infrastruttura sottostante (ad esempio, VMware), l'utilizzo di queste risorse verrà regolato per garantire il conteggio più efficiente delle unità gestite. È possibile visualizzare le modifiche apportate a Kubernetes MU nella pagina Amministrazione > Abbonamento, nelle schede Riepilogo e Utilizzo.

Scheda
Riepilogo:



Scheda
Utilizzo:



Modifiche al collezionista/acquisizione:

Sono in atto le seguenti modifiche all'unità di raccolta/acquisizione dati:

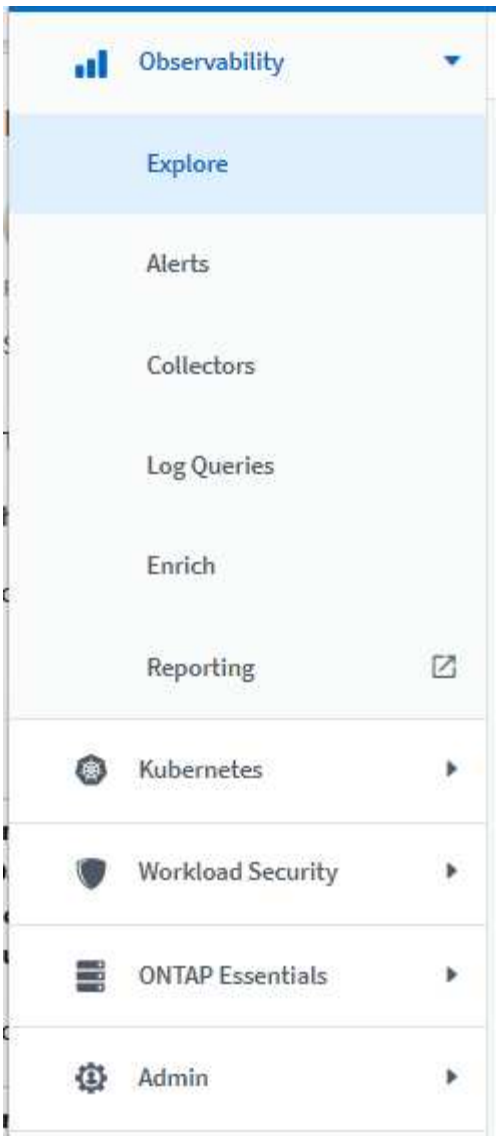
- Le unità di acquisizione ora supportano RHEL 8.7.

Menu migliorati

Abbiamo aggiornato il menu di navigazione a sinistra per supportare meglio i flussi di lavoro dei nostri clienti. Nuovi elementi di primo livello come *Kubernetes* forniscono un accesso accelerato a ciò di cui il cliente ha bisogno, mentre una console di amministrazione consolidata supporta il ruolo di proprietario del tenant.

Ecco alcuni esempi aggiuntivi delle modifiche:

- Il menu di livello superiore *Observability* mostra la scoperta dei dati, gli avvisi e le query di registro
- Le funzionalità di "Accesso API" per l'osservabilità e la sicurezza del carico di lavoro sono raggruppate in un unico menu
- Allo stesso modo, per la funzionalità "Notifiche" di Osservabilità e Sicurezza del Carico di Lavoro, ora anche in un unico menu



Ecco un breve elenco delle funzionalità che puoi trovare in ciascun menu:

Osservabilità:

- Esplora (Dashboard, query sulle metriche, approfondimenti sull'infrastruttura)
- Avvisi (monitor e avvisi)
- Collezionisti (collettori di dati e unità di acquisizione)
- Query di registro
- Arricchisci (Annotazioni e regole di annotazione, Applicazioni, Risoluzione del dispositivo)
- Segnalazione

Kubernetes:

- Esplorazione dei cluster e mappa della rete

Sicurezza del carico di lavoro:

- Avvisi

- Medicina legale
- Collezionisti
- Politiche

Elementi essenziali ONTAP :

- Protezione dei dati
- Sicurezza
- Avvisi
- Infrastruttura
- Networking
- Carichi di lavoro *VMware

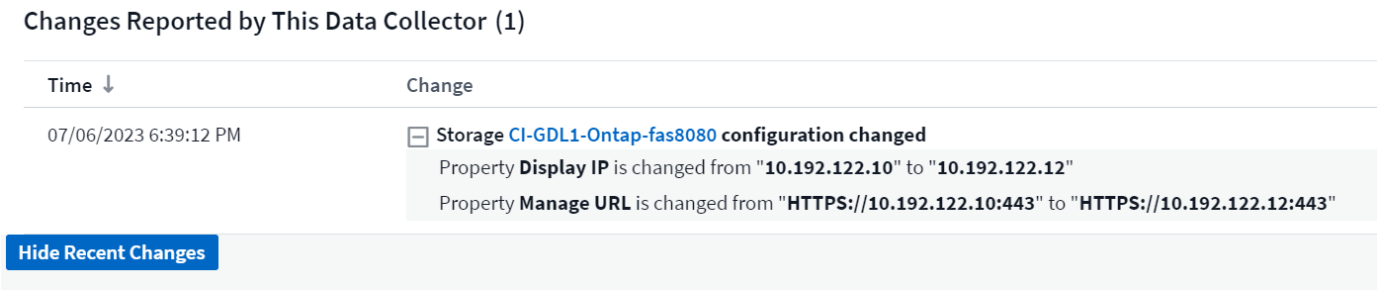
Amministratore:

- Accesso API
- Revisione contabile
- Notifiche
- Informazioni sull'abbonamento
- Gestione degli utenti

Luglio 2023

Mostra modifiche recenti

Le landing page di Data Collector ora includono un elenco delle modifiche recenti. Basta cliccare sul pulsante "Modifiche recenti" in fondo a qualsiasi pagina di destinazione del raccoglitore dati per visualizzare le modifiche recenti apportate al raccoglitore dati.



Miglioramenti dell'operatore

Sono stati apportati i seguenti miglioramenti"Operatore Kubernetes" distribuzione:

- Opzione per ignorare la raccolta delle metriche Docker
- Possibilità di aggiungere e personalizzare le tolleranze ai Daemonset e ai Replicaset di Telegraf

Approfondimento: Recuperare lo stoccaggio a freddo

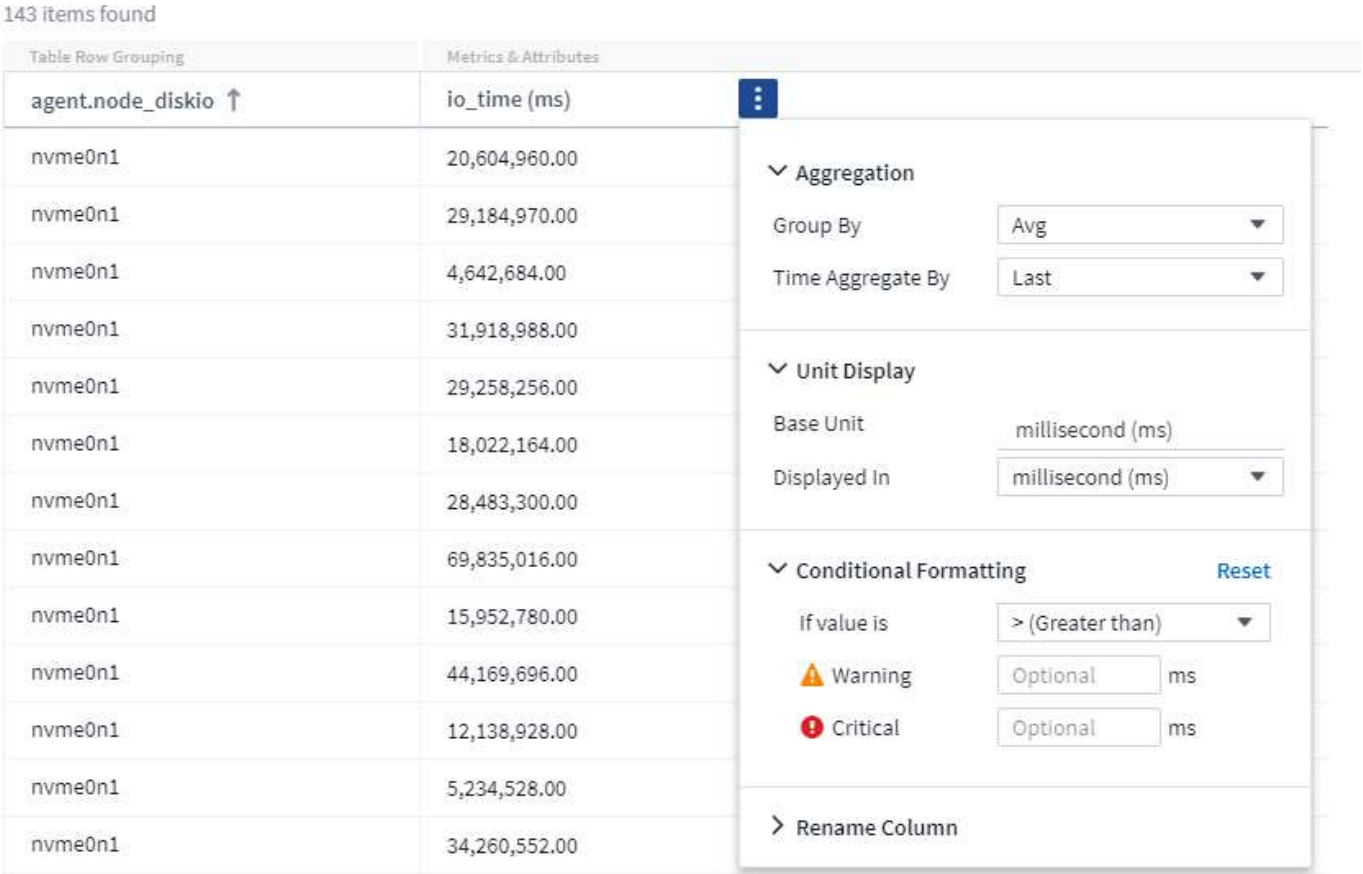
IL"Reclaim ONTAP Cold Storage Insight" ora supporta FlexGroups ed è disponibile per tutti i clienti.

Firma dell'immagine dell'operatore

Per i clienti che utilizzano un repository privato per il loro NetApp Kubernetes Monitoring Operator, ora è possibile copiare la chiave pubblica della firma dell'immagine durante l'installazione dell'operatore, consentendo di confermare l'autenticità del software scaricato. Selezionare il pulsante *Copia chiave pubblica della firma dell'immagine* durante il passaggio facoltativo per *Caricare l'immagine dell'operatore nel repository privato*.

Aggregazione, formattazione condizionale e altro per le query

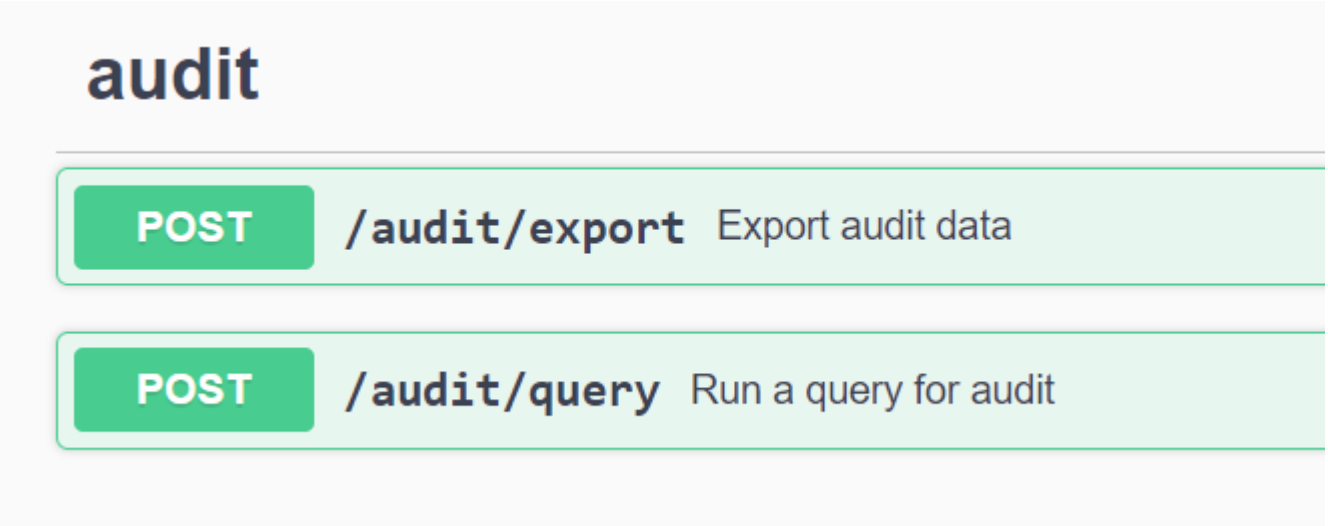
Aggregazione, selezione unità, formattazione condizionale e ridenominazione colonne sono tra le funzionalità più utili di un widget tabella dashboard e ora le stesse funzionalità sono disponibili per"Query" .



Queste funzionalità sono ora disponibili per i dati di tipo integrazione (Kubernetes, ONTAP Advanced Metrics, ecc.) e saranno presto disponibili anche per gli oggetti dell'infrastruttura (archiviazione, volume, switch, ecc.).

API per l'audit

Ora puoi utilizzare un'API per interrogare o esportare gli eventi controllati. Vai su Amministrazione > Accesso API e seleziona il link *Documentazione API* per informazioni.



Raccolta dati: Trident Economy

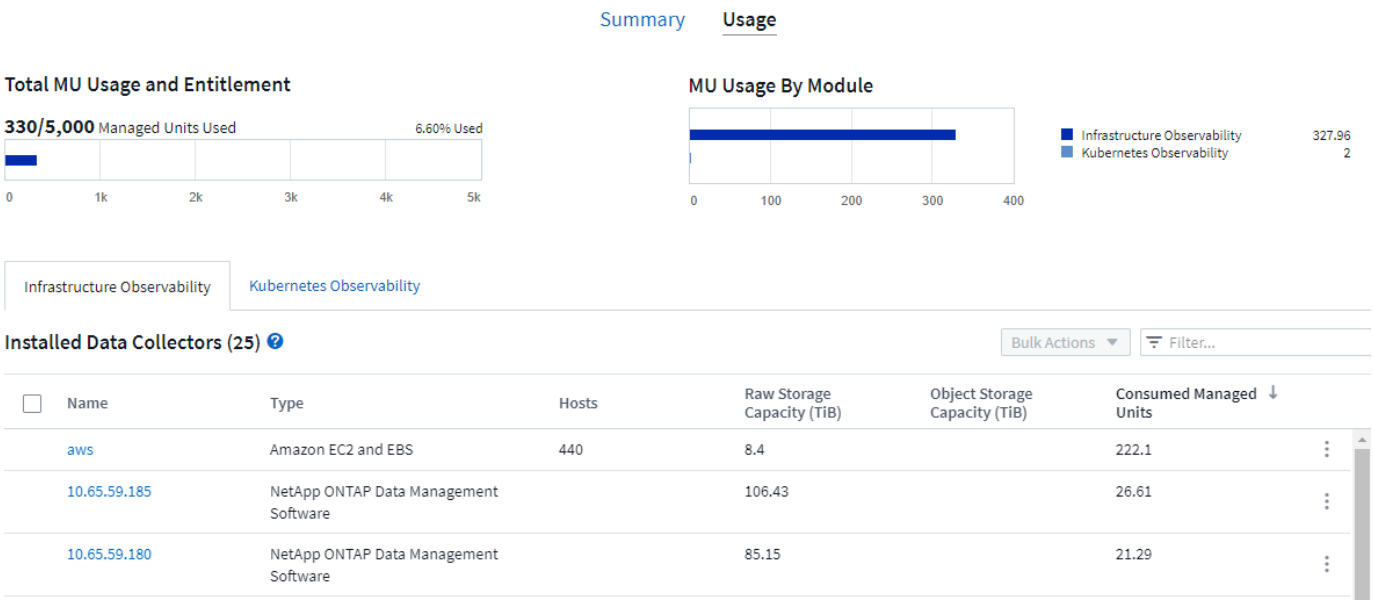
Cloud Insights ora supporta Trident Economy Driver, realizzando i seguenti vantaggi:

- Ottieni visibilità sulla mappatura Qtree pod-to- ONTAP e sulle metriche delle prestazioni.
- Fornire una risoluzione dei problemi senza interruzioni e una navigazione semplice dai pod Kubernetes allo storage back-end
- Rileva proattivamente i problemi di prestazioni del backend con i monitor

Giugno 2023

Controlla il tuo utilizzo

A partire da giugno 2023, Cloud Insights fornirà una ripartizione dell'utilizzo delle unità gestite in base al set di funzionalità. Ora puoi visualizzare e monitorare rapidamente l'utilizzo delle unità gestite (MU) per la tua infrastruttura, nonché l'utilizzo delle MU associato a Kubernetes.



Il monitoraggio e la mappa della rete Kubernetes sono disponibili per tutti

IL"*Prestazioni e mappa della rete Kubernetes*" Semplifica la risoluzione dei problemi mappando le dipendenze tra i carichi di lavoro di Kubernetes, offrendo visibilità in tempo reale sulle latenze e sulle anomalie delle prestazioni della rete Kubernetes per identificare i problemi di prestazioni prima che influiscano sugli utenti. Molti clienti l'hanno trovato utile durante l'anteprima e ora è disponibile per tutti.

Modifiche al collezionista/acquisizione:

Sono in atto le seguenti modifiche all'unità di raccolta/acquisizione dati:

- Le MU di Data Domain e Cohesity sono misurate a 40 TiB: 1 MU.
- Le unità di acquisizione ora supportano RHEL e Rocky 9.0 e 9.1.

Nuove dashboard ONTAP Essentials

Le seguenti dashboard di ONTAP Essentials erano disponibili negli ambienti di anteprima e ora sono disponibili per tutti:

- Pannello di controllo della sicurezza
- Dashboard sulla protezione dei dati (include panoramiche sulla protezione locale e remota)

Monitor di sistema aggiuntivi

I seguenti monitor di sistema sono inclusi in Cloud Insights:

- Servizio FCP VM di archiviazione non disponibile
- Servizio iSCSI VM di archiviazione non disponibile

Maggio 2023

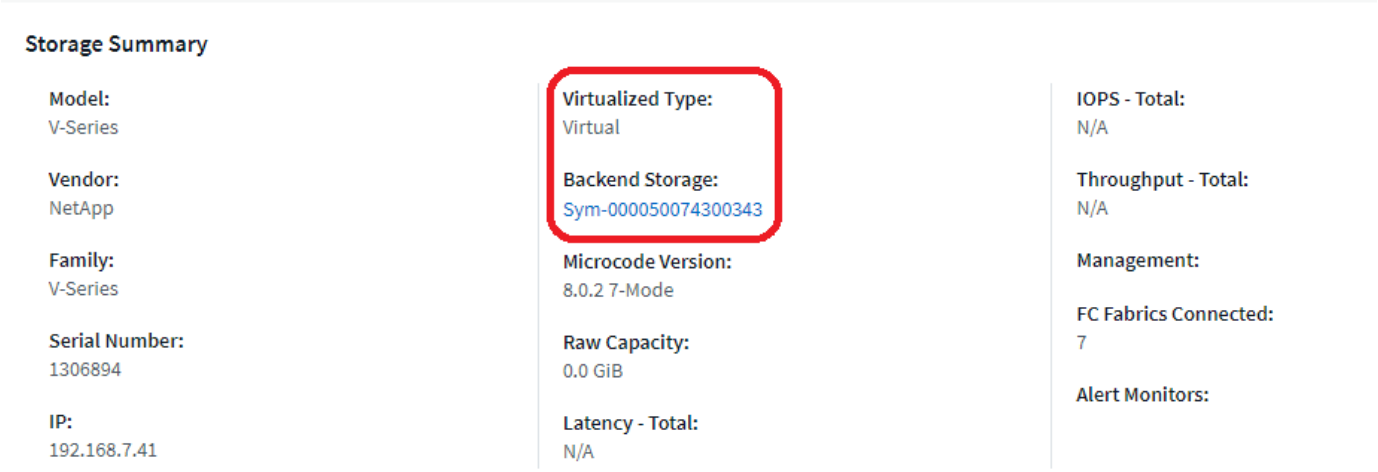
Installazione migliorata dell'operatore di monitoraggio Kubernetes

Installazione e configurazione del"Operatore di monitoraggio NetApp Kubernetes" è più facile che mai con i seguenti miglioramenti:

- Ambiente"impostazioni di configurazione" sono contenuti in un unico file di configurazione autodocumentato.
- Istruzioni dettagliate per caricare le immagini di Kubernetes Monitoring Operator nel tuo repository privato.
- Semplice da aggiornare con un singolo comando per aggiornare il tuo Kubernetes Monitoring mantenendo le configurazioni personalizzate.
- Maggiore sicurezza: le chiavi API gestiscono i segreti in modo sicuro.
- Facile da integrare e distribuire con i tuoi strumenti di automazione CI/CD.

Virtualizzazione dello storage

Cloud Insights è in grado di distinguere tra un array di storage con storage locale e la virtualizzazione di altri array di storage. Ciò ti consente di mettere in relazione i costi e di distinguere le prestazioni dal front-end fino al back-end della tua infrastruttura.



Nuovi parametri webhook

Quando si crea un"Webhook" notifica, ora puoi includere questi parametri nella definizione del tuo webhook:

- %%TriggeredOnKeys%%
- %%TriggeredOnValues%%

Report sui dati di Kubernetes

I dati Kubernetes raccolti da Cloud Insights, tra cui Persistent Volumes (PV), PVC, Workloads, Cluster e Namespace, sono ora disponibili per l'utilizzo in Reporting, consentendo chargeback, trending, forecasting, calcoli TTF e altri report aziendali sulle metriche per Kubernetes.

Monitor di sistema ONTAP predefiniti abilitati per i nuovi clienti

Molti monitor di sistema ONTAP sono abilitati (ovvero *Ripresi*) per impostazione predefinita nei nuovi ambienti Cloud Insights . In precedenza, la maggior parte dei monitor era impostata sullo stato *Paused* (in pausa). Poiché le esigenze aziendali variano da azienda ad azienda, consigliamo sempre di dare un'occhiata al"monitor di sistema" nel tuo ambiente e sospendendo o riprendendo ciascuna di esse in base alle tue esigenze di avviso.

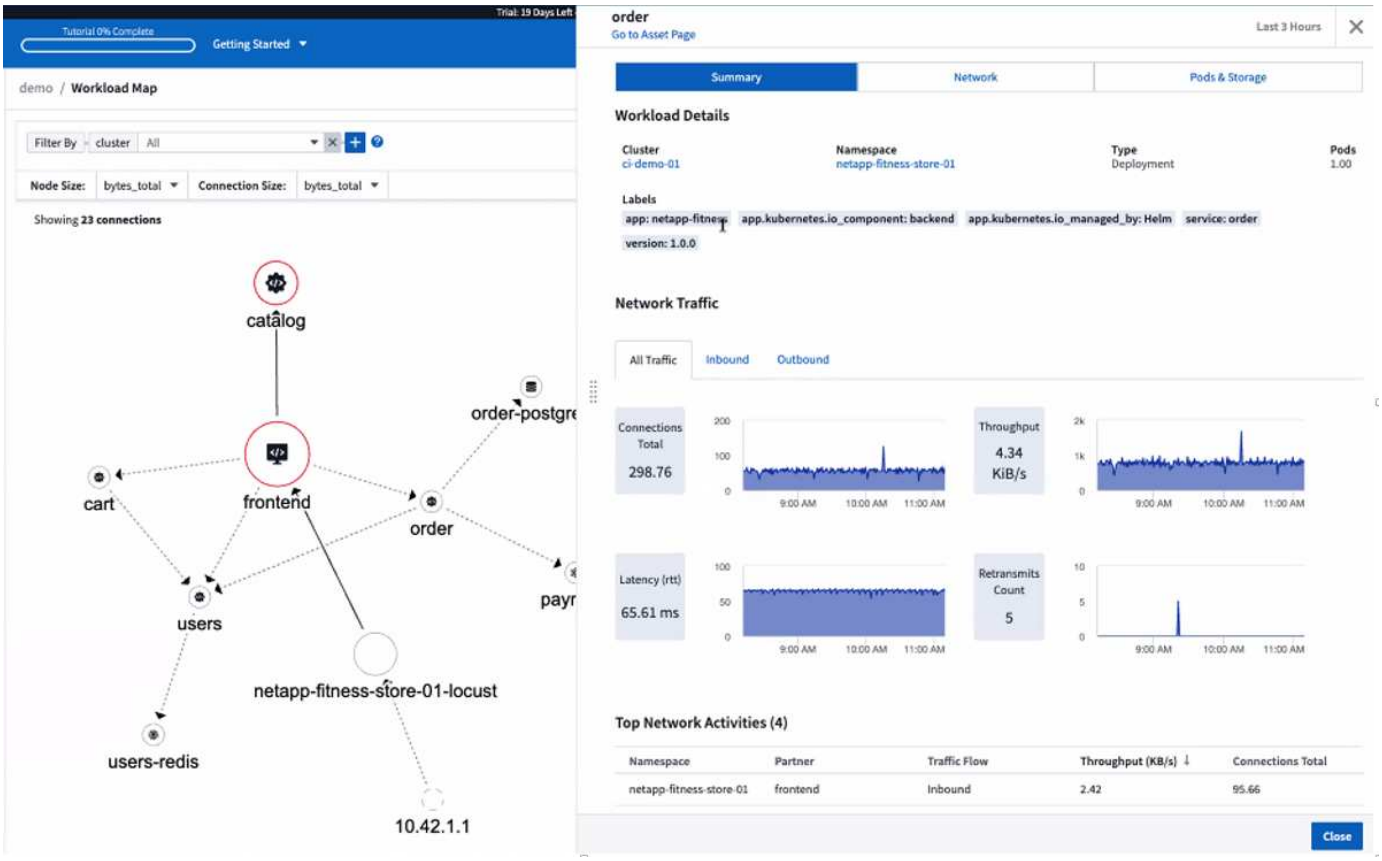
Aprile 2023

Monitoraggio e mappa delle prestazioni di Kubernetes

IL"*Prestazioni e mappa della rete Kubernetes*" La funzionalità semplifica la risoluzione dei problemi mappando le dipendenze tra i carichi di lavoro Kubernetes. Fornisce visibilità in tempo reale sulle latenze e sulle anomalie delle prestazioni della rete Kubernetes per identificare i problemi di prestazioni prima che influiscano sugli utenti. Questa funzionalità aiuta le organizzazioni a ridurre i costi complessivi analizzando e verificando i flussi di traffico di Kubernetes.

Caratteristiche principali: • La mappa del carico di lavoro presenta le dipendenze e i flussi del carico di lavoro di Kubernetes e mette in evidenza i problemi di rete e prestazioni. • Monitora il traffico di rete tra pod, carichi di lavoro e nodi Kubernetes; identifica l'origine del traffico e i problemi di latenza. • Ridurre i costi complessivi analizzando il traffico di rete in ingresso, in uscita, tra regioni e tra zone.

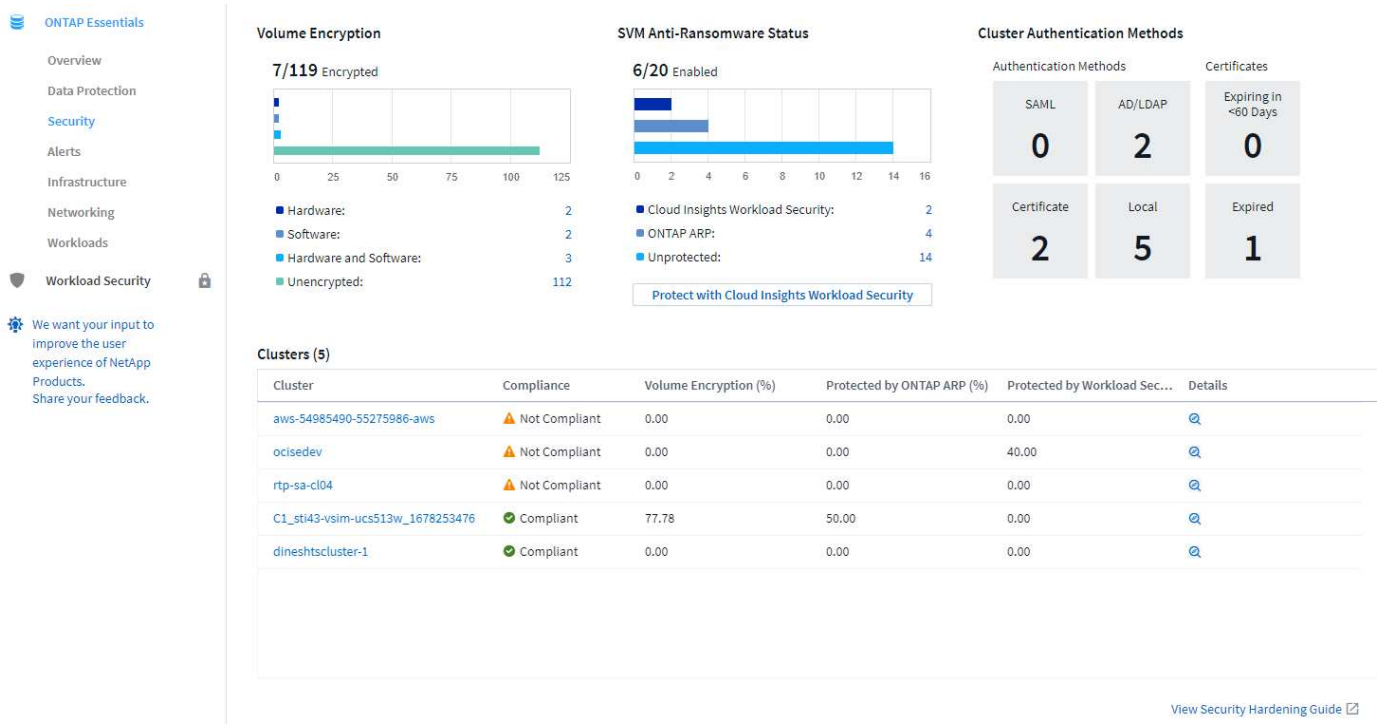
Mappa del carico di lavoro che mostra i dettagli di "Slideout":



Kubernetes Performance Monitoring and Map è disponibile come"Anteprima" caratteristica.

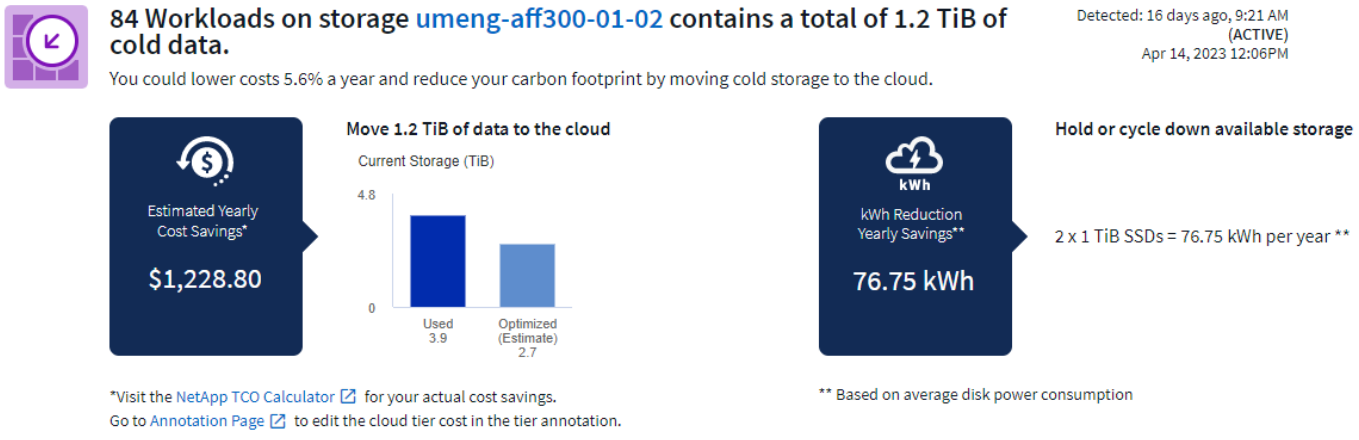
Pannello di controllo di sicurezza ONTAP Essentials

IL"Pannello di controllo della sicurezza" fornisce una panoramica immediata della situazione attuale della sicurezza, mostrando grafici relativi alla crittografia dei volumi hardware e software, allo stato anti-ransomware e ai metodi di autenticazione del cluster. Il Security Dashboard è disponibile come"Anteprima" caratteristica.



Reclaim ONTAP Cold Storage

Reclaim ONTAP Cold Storage Insight fornisce dati sulla capacità di raffreddamento, sui potenziali risparmi in termini di costi/energia e sulle azioni consigliate per i volumi sui sistemi ONTAP .



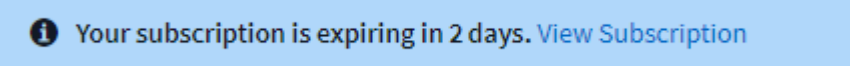
Grazie a questa Insight, puoi rispondere a domande come:

- Quanta quantità di dati inattivi su un cluster di storage si trova su (a) costosi dischi SSD, (b) dischi HDD e (c) dischi virtuali?
- Quali carichi di lavoro contribuiscono maggiormente allo storage non ottimizzato?
- Per quanto tempo (in giorni) i dati sono rimasti inattivi in un dato carico di lavoro?

Reclaim ONTAP Cold Storage è considerato un"*Anteprima*" caratteristica ed è pertanto soggetta a modifiche.

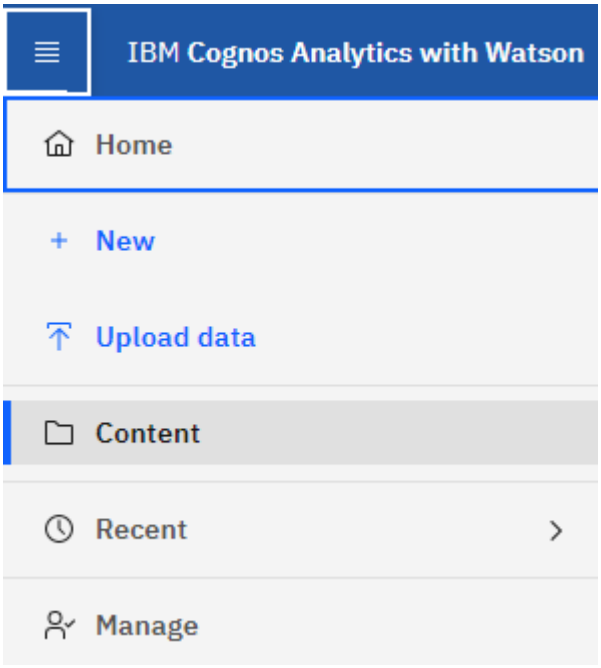
La notifica di abbonamento controlla anche i messaggi banner

L'impostazione dei destinatari per le notifiche di abbonamento (Amministrazione > Notifiche) ora controlla anche chi visualizzerà le notifiche banner all'interno del prodotto relative all'abbonamento.



Il reporting ha un nuovo aspetto

Noterai che le schermate di Cloud Insights Reporting hanno un nuovo aspetto e che alcuni elementi del menu di navigazione sono cambiati. Queste schermate e le modifiche alla navigazione sono state aggiornate nella versione corrente"Documentazione di segnalazione" .



Monitor in pausa per impostazione predefinita

Per i nuovi ambienti Cloud Insights , tieni presente che"monitor definiti dal sistema" non inviare notifiche di avviso per impostazione predefinita. Sarà necessario abilitare le notifiche per ogni monitor da cui si desidera ricevere avvisi, aggiungendo uno o più metodi di consegna per il monitor. Per gli ambienti Cloud Insights esistenti, l'elenco predefinito dei destinatari delle notifiche *globali* è stato rimosso per tutti i monitor definiti dal sistema attualmente in stato *Sospeso*. Le notifiche definite dall'utente rimangono invariate, così come le impostazioni di notifica per i monitor definiti dal sistema attualmente attivi.

Cerchi la scheda Misurazione API?

La misurazione API è stata spostata dalla pagina Abbonamento alla pagina **Amministrazione > Accesso API**.

Marzo 2023

Connessione cloud per ONTAP 9.9+ obsoleta

La connessione Cloud per il raccoglitore dati ONTAP 9.9+ è obsoleta. A partire dal 4 aprile 2023, i raccoglitori di dati Cloud Connection nel tuo ambiente non raccoglieranno più dati e visualizzeranno un errore durante il polling. Il raccoglitore di dati Cloud Connection verrà rimosso completamente da Cloud Insights in un aggiornamento successivo.

Prima del 4 aprile 2023, è obbligatorio configurare un nuovo raccoglitore dati NetApp ONTAP Data Management Software per tutti i sistemi ONTAP attualmente raccolti da Cloud Connection.

Gennaio 2023

Nuovi monitor di registro

Ne abbiamo aggiunti quasi due dozzine"monitor di sistema aggiuntivi" per avvisare in caso di collegamenti di interconnessione interrotti, problemi di heartbeat e altro ancora. Sono stati inoltre aggiunti tre nuovi monitor di log sulla protezione dei dati per avvisare sulle modifiche di SnapMirror Auto Resync, MetroCluster Mirroring e FabricPool Mirror Resync.

Tieni presente che alcuni di questi monitor saranno *abilitati* per impostazione predefinita; devi metterli in *pausa* se non desideri ricevere avvisi. Si noti inoltre che questi monitor non sono configurati per inviare notifiche; è necessario configurare i destinatari delle notifiche su questi monitor se si desidera inviare avvisi tramite e-mail o webhook.

Esportazione .CSV per tutti i widget della tabella della dashboard

Garantire l'accessibilità ai dati è essenziale, per questo abbiamo reso disponibile l'esportazione in formato .CSV per tutte le query di metriche, i widget delle tabelle della dashboard e le landing page degli oggetti, indipendentemente dal tipo di dati (risorsa o integrazione) che stai interrogando.

Anche le personalizzazioni dei dati, come la selezione delle colonne, la ridenominazione delle colonne e la conversione delle unità, sono ora incluse nella nuova funzionalità di esportazione.

Dicembre 2022

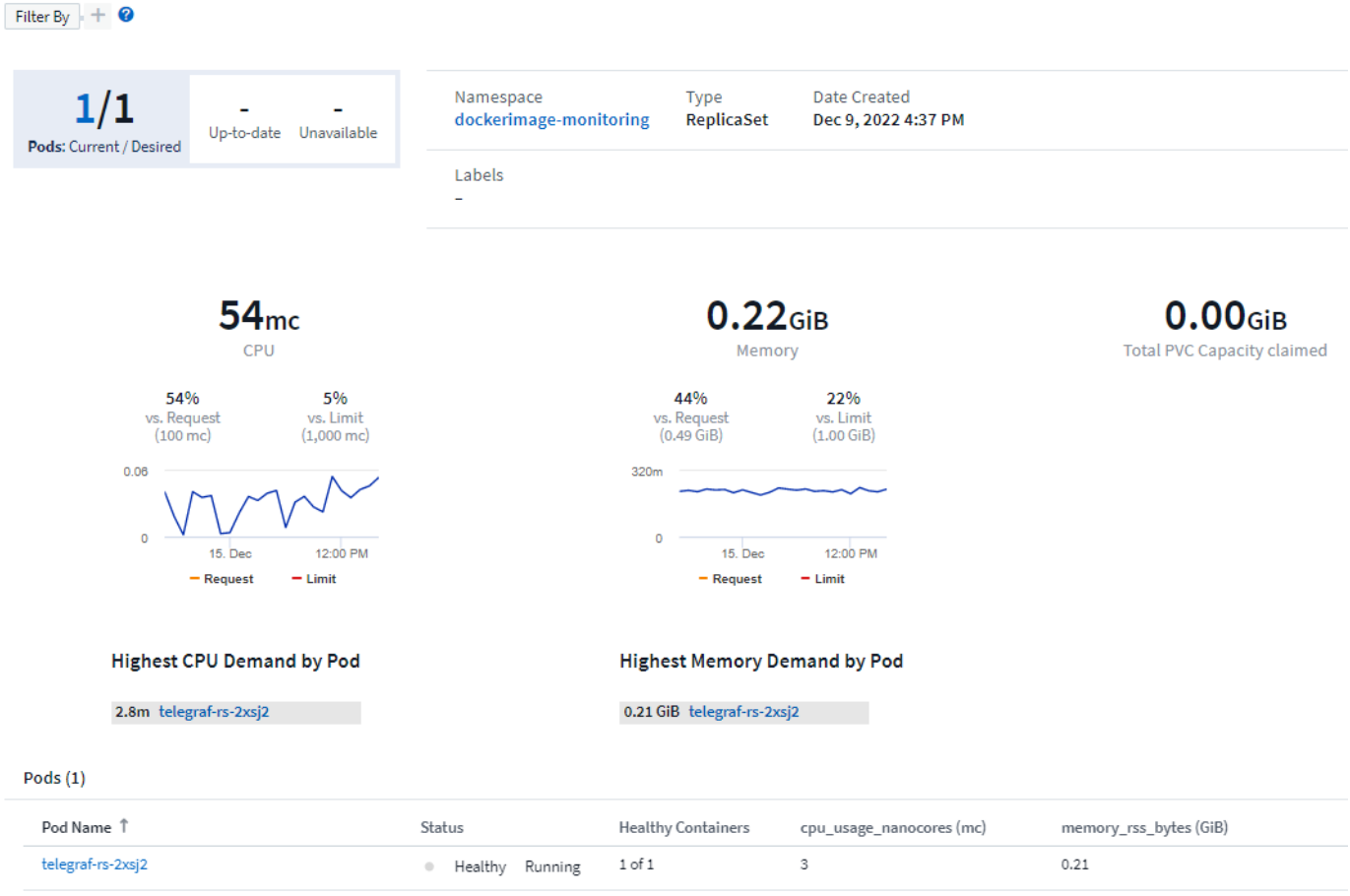
Scopri la protezione dal ransomware e altre funzionalità di sicurezza durante la prova Cloud Insights

A partire da oggi, registrandoti per una nuova prova di Cloud Insights potrai esplorare funzionalità di sicurezza come il rilevamento di ransomware e la politica di risposta automatica al blocco degli utenti. Se non ti sei ancora registrato per la tua prova gratuita, fallo oggi stesso!

I carichi di lavoro Kubernetes hanno la loro landing page

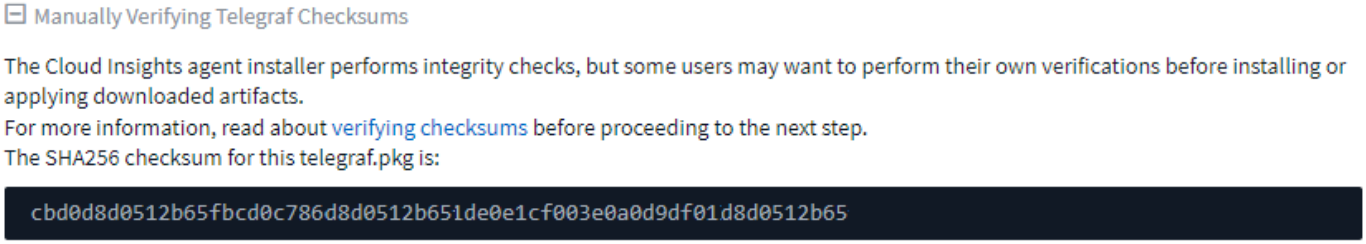
I carichi di lavoro sono una parte fondamentale del tuo ambiente Kubernetes, per questo Cloud Insights ora fornisce landing page per tali carichi di lavoro. Da qui puoi visualizzare, esplorare e risolvere i problemi che

interessano i tuoi carichi di lavoro Kubernetes.



Controlla i tuoi checksum

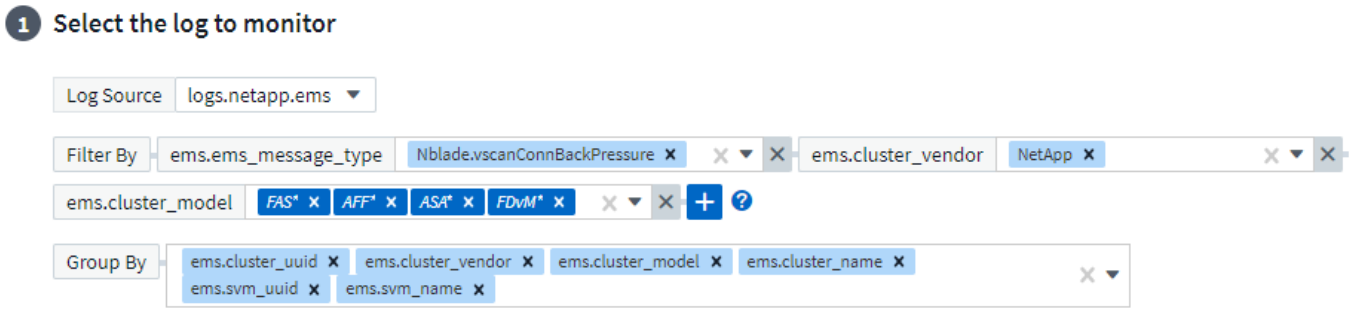
Ci avete chiesto di fornirvi i valori di checksum durante l'installazione dell'agente per Windows e Linux e pensiamo che sia un'ottima idea. Eccole qui:



Miglioramenti degli avvisi di registro

Raggruppa per

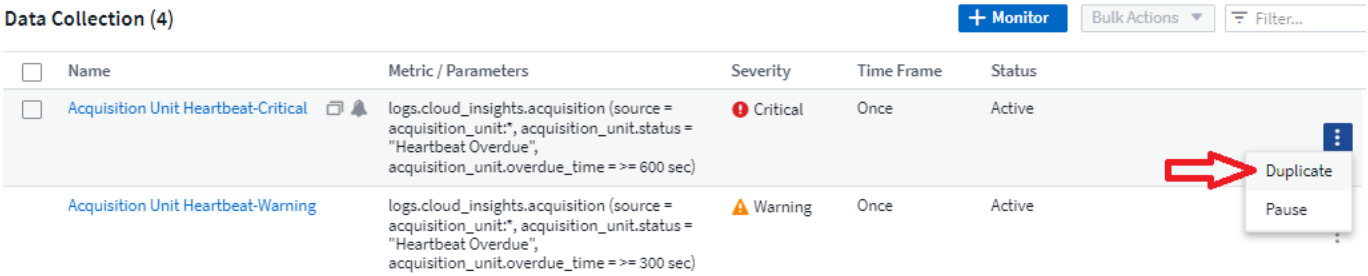
Quando si crea o si modifica un Log Monitor, ora è possibile impostare gli attributi "Raggruppa per" per consentire avvisi più mirati. Cerca gli attributi "Raggruppa per" sotto le impostazioni "filtro" nella definizione del monitor.



Questa modifica porta i monitor delle metriche e i monitor dei log alla parità di funzionalità normalizzando l'aspetto "Raggruppa per" delle definizioni dei monitor. Questa parità consentirà ai clienti di clonare/duplicare **tutti** i monitor predefiniti definiti dal sistema per un'ulteriore personalizzazione.

Duplicazione

Ora puoi clonare (duplicare) i monitor Change Log, Kubernetes Log e Data Collector Log. In questo modo viene creato un nuovo monitor di log personalizzato che puoi modificare in base alle tue specifiche definizioni.



11 nuovi monitor ONTAP predefiniti che coprono SnapMirror per la continuità aziendale

Abbiamo aggiunto quasi una dozzina di nuovi"monitor di sistema" per SnapMirror for Business Continuity (SMBC), che avvisa sulle modifiche ai certificati SMBC e ai mediatori ONTAP .

Novembre 2022

Oltre 40 nuovi monitor di sicurezza, raccolta dati e CVO!

Abbiamo aggiunto decine di nuovi monitor definiti dal sistema per avvisarti di potenziali problemi con Cloud Volumes, sicurezza e protezione dei dati. Scopri di più su questi monitor"Qui" .

Ottobre 2022

Rilevamento ransomware migliore e più accurato con l'integrazione di ONTAP Autonomous Ransomware Protection

Cloud Secure migliora il rilevamento del ransomware tramite l'integrazione con ONTAP"Protezione autonoma

dal ransomware" (ARP).

Cloud Secure riceve eventi ONTAP ARP su potenziali attività di crittografia dei file di volume e

- Correla gli eventi di crittografia del volume con l'attività dell'utente per identificare chi sta causando il danno,
- Implementa politiche di risposta automatica per bloccare l'attacco,
- Identifica i file interessati, contribuendo a un recupero più rapido e a condurre indagini sulle violazioni dei dati.

Settembre 2022

Monitor disponibili in Basic Edition

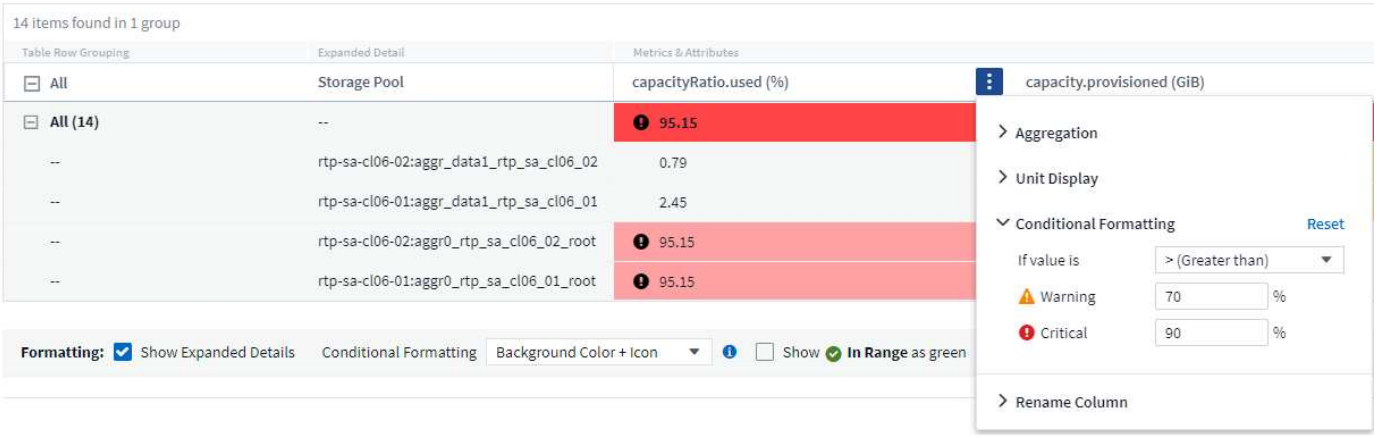
ONTAP"Monitor predefiniti" ora disponibile per l'uso in Cloud Insights Basic Edition. Ciò include più di 70 monitor dell'infrastruttura e 30 esempi di carichi di lavoro.

Dashboard ONTAP Power e StorageGRID

La galleria dashboard include una nuova dashboard per ONTAP Power e Temperature, nonché quattro dashboard per StorageGRID. Se il tuo ambiente raccoglie metriche di potenza ONTAP e/o dati StorageGRID , importa queste dashboard selezionando **+Da Galleria**.

Visibilità immediata della soglia nelle tabelle

La formattazione condizionale consente di impostare ed evidenziare le soglie di livello di avviso e di livello critico nei widget della tabella, offrendo visibilità immediata ai valori anomali e ai punti dati eccezionali.



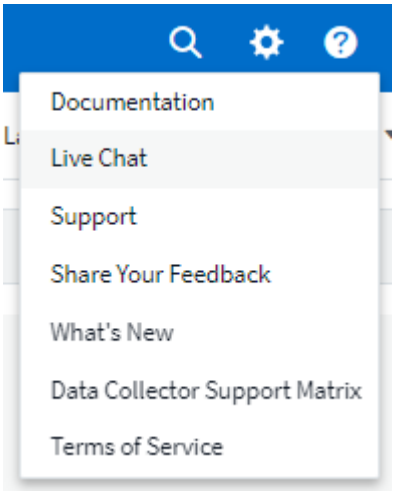
Monitor di sicurezza

Cloud Insights può avvisarti quando rileva che la modalità FIPS è disabilitata sul sistema ONTAP . Per saperne di più"Monitor di sistema" e continuate a seguirci per altri Security Monitor in arrivo prossimamente!

Chatta da qualsiasi luogo

Chatta con uno specialista del supporto NetApp da qualsiasi schermata Cloud Insights selezionando il nuovo

collegamento **Aiuto > Chat in tempo reale**. Per ottenere assistenza, fai clic sull'icona "?" in alto a destra dello schermo.



Approfondimenti più visibili

Se il tuo ambiente sta vivendo un"Intuizione" come *Risorse condivise sotto stress* o *Spazio dei nomi Kubernetes in esaurimento*, le landing page delle risorse interessate ora includono link all'Insight stesso, consentendo un'esplorazione e una risoluzione dei problemi più rapide.

Nuovi raccoglitori di dati

- Amazon S3 (disponibile in anteprima)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Altri aggiornamenti del Data Collector

Tutte le fonti di dati sono ora ottimizzate per riprendere il polling delle prestazioni dopo gli aggiornamenti e/o le patch dell'unità di acquisizione.

Supporto del sistema operativo

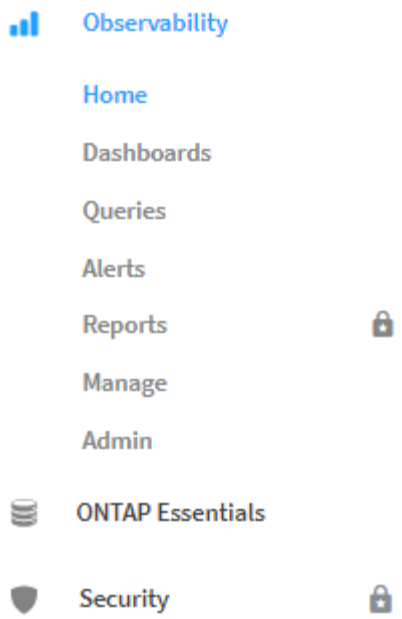
Oltre a quelli supportati da Cloud Insights Acquisition Units, sono supportati anche i seguenti sistemi operativi:"già supportato" :

- Red Hat Enterprise Linux 8.5, 8.6

Agosto 2022

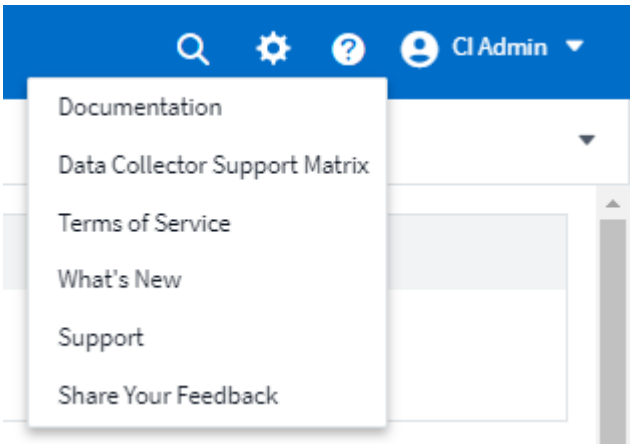
Cloud Insights ha un nuovo look!

A partire da questo mese, "Monitoraggio e ottimizzazione" è stato rinominato **Osservabilità**. Qui troverai tutte le tue funzionalità preferite, come Dashboard, Query, Avvisi e Report. Inoltre, cerca Cloud Secure nel nuovo menu **Sicurezza**. Da notare che sono cambiati solo i menu; le funzionalità rimangono le stesse.



Cerchi il menu **Aiuto**?

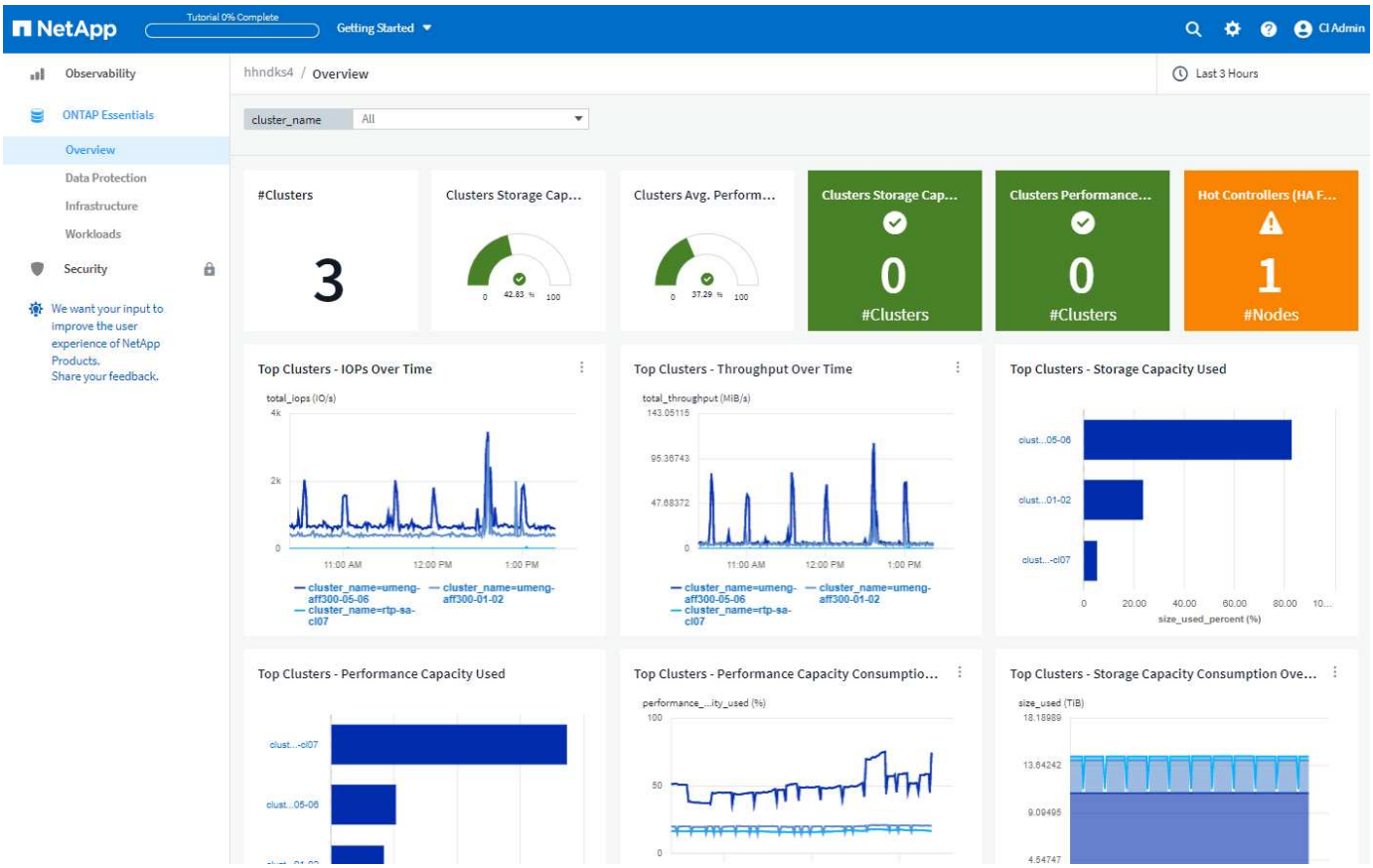
Ora la guida si trova in alto a destra dello schermo.



Non sai da dove iniziare? Scopri ONTAP Essentials!

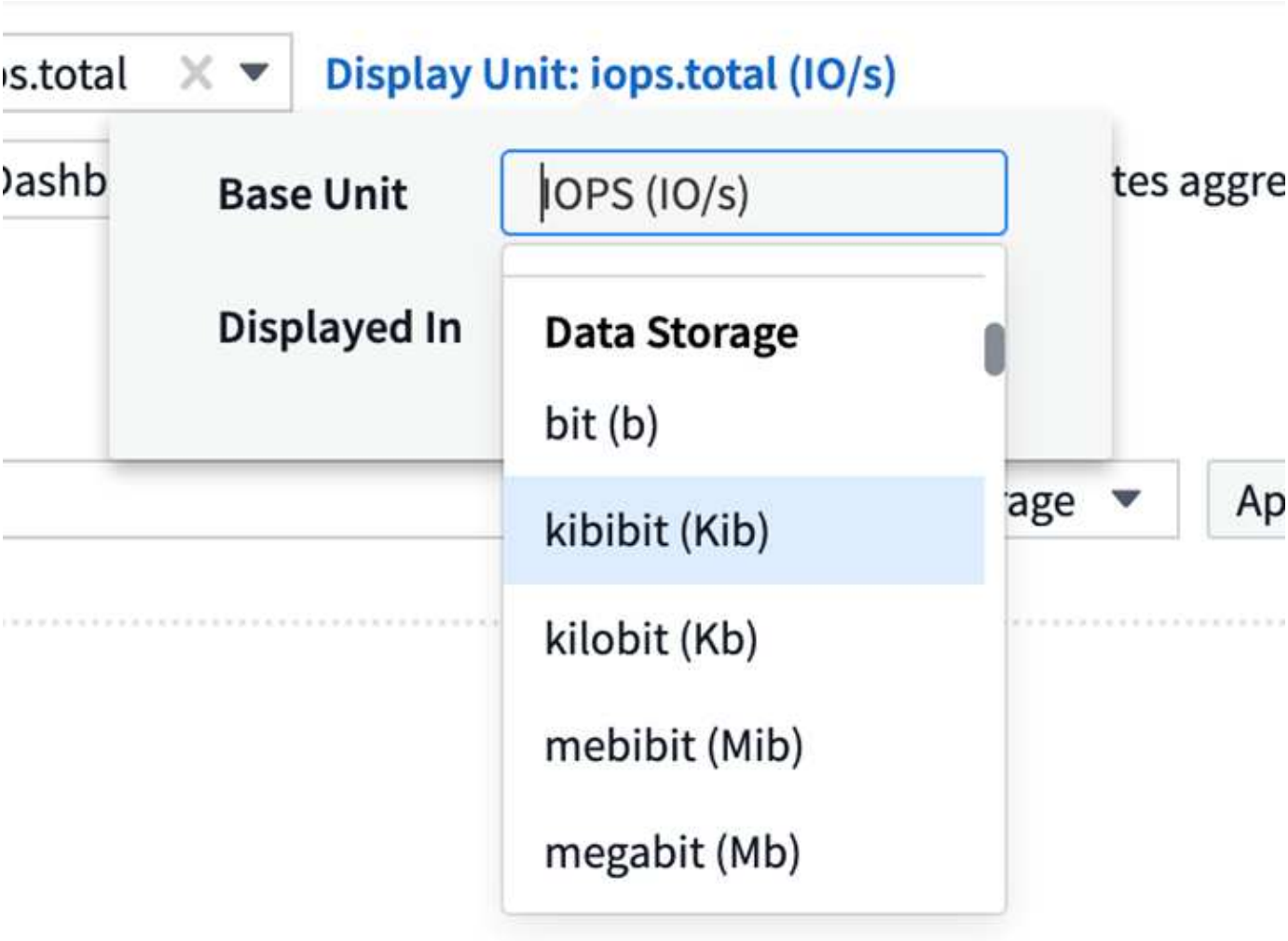
"* Elementi essenziali ONTAP *"è un set di dashboard e flussi di lavoro che forniscono viste dettagliate degli inventari, dei carichi di lavoro e della protezione dei dati NetApp ONTAP , comprese previsioni di giorni di utilizzo completo per capacità e prestazioni di storage. È anche possibile verificare se alcuni controller sono in esecuzione con un utilizzo elevato. ONTAP Essentials è il punto di riferimento ideale per tutte le tue esigenze di monitoraggio NetApp ONTAP !

ONTAP Essentials, disponibile in tutte le edizioni, è progettato per essere intuitivo per gli attuali operatori e amministratori ONTAP , semplificando la transizione da ActiveIQ Unified Manager agli strumenti di gestione basati sui servizi.



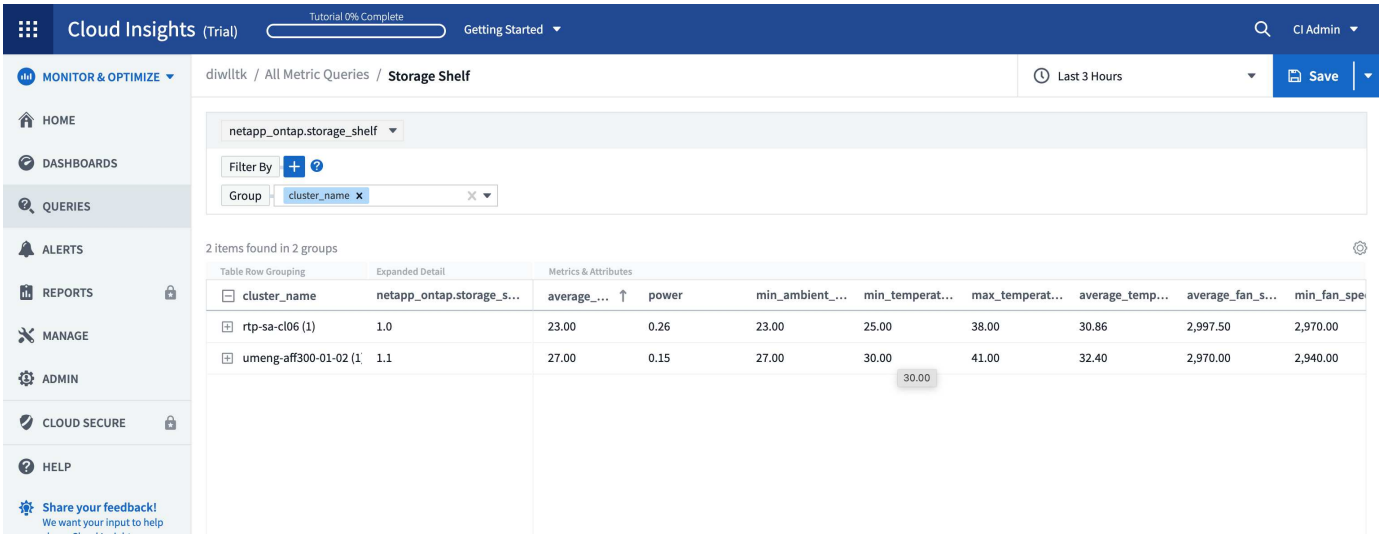
Le famiglie di dati di archiviazione vengono unite

L'avete chiesto e ora ce l'avete ottenuto. Le unità di dati di archiviazione base 2 e base 10 sono ora combinate in un'unica famiglia, da bit e byte a tebibit e terabyte, semplificando la visualizzazione dei dati sulle dashboard. Anche le velocità dei dati costituiscono ormai una grande famiglia a sé stante.



Quanta energia consuma il mio storage?

Visualizza e monitora il consumo energetico, la temperatura e la velocità della ventola dello storage shelf e del nodo ONTAP , utilizzando le metriche netapp_ontap.storage_shelf, netapp_ontap.system_node e netapp_ontap.cluster (solo consumo energetico).



Funzionalità graduate da Anteprima

Le seguenti funzionalità sono state rimosse dalla versione Preview e sono ora disponibili per tutti i clienti:

Caratteristica	Descrizione
Gli spazi dei nomi di Kubernetes stanno esaurendo lo spazio	L'Insight *Kubernetes Namespaces Running Out of Space* fornisce una panoramica dei carichi di lavoro sui namespace Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si riempia."Per saperne di più"
Risorsa condivisa sotto stress	L'insight *Shared Resource Under Stress* utilizza l'intelligenza artificiale e l'apprendimento automatico per identificare automaticamente dove la contesa delle risorse sta causando un degrado delle prestazioni nel tuo ambiente, evidenzia tutti i carichi di lavoro interessati e fornisce azioni consigliate per porvi rimedio, consentendoti di risolvere i problemi di prestazioni più rapidamente."Per saperne di più"
Cloud Secure : blocca l'accesso degli utenti in caso di attacco	Maggiore protezione per i dati aziendali critici con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando i criteri di risposta automatica, oppure manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Per saperne di più"

Come sta andando la mia raccolta dati?

Cloud Insights fornisce due nuovi monitor heartbeat per le tue unità di acquisizione, nonché due monitor per avvisarti di eventuali guasti del raccoglitore dati. Possono essere utilizzati per avvisarti rapidamente di eventuali problemi di raccolta dati.

I seguenti monitor sono ora disponibili nel gruppo di monitor *Raccolta dati*:

- Unità di acquisizione Heartbeat-Critical
- Avviso di battito cardiaco dell'unità di acquisizione
- Collettore fallito
- Avviso al collezionista

Si noti che per impostazione predefinita questi monitor sono in stato *In pausa*. Attivali per essere avvisato sui problemi di raccolta dati.

Token API con rinnovo automatico

Ora è possibile impostare il rinnovo automatico dei token di accesso API. Abilitando questa funzionalità, verranno generati automaticamente nuovi/aggiornati token di accesso API per i token in scadenza. Gli agenti Cloud Insights che utilizzano un token in scadenza verranno automaticamente aggiornati per utilizzare il token di accesso API nuovo/aggiornato corrispondente, consentendo loro di continuare a funzionare senza problemi. Basta selezionare la casella "Rinnova automaticamente il token" quando crei il tuo token. Questa funzionalità è attualmente supportata sugli agenti Cloud Insights in esecuzione sulla piattaforma Kubernetes con la versione

più recente di NetApp Kubernetes Monitoring Operator.

La Basic Edition ti offre più di prima

Il tuo periodo di prova sta per scadere ma non sei ancora sicuro che l'abbonamento sia adatto a te? La Basic Edition ti ha sempre dato la possibilità di continuare a utilizzare Cloud Insights con il tuo attuale raccoglitore dati ONTAP , ma ora puoi continuare ad acquisire anche i dati relativi a versione, topologia e IOPS/throughput/latenza di VMWare. I clienti NetApp con supporto premium sui loro sistemi di storage avranno diritto anche al supporto per Cloud Insights.

Pronti a saperne di più?

Consulta la sezione **Centro di apprendimento** della pagina Aiuto > Supporto per i link ai corsi offerti da NetApp University Cloud Insights !

Supporto del sistema operativo

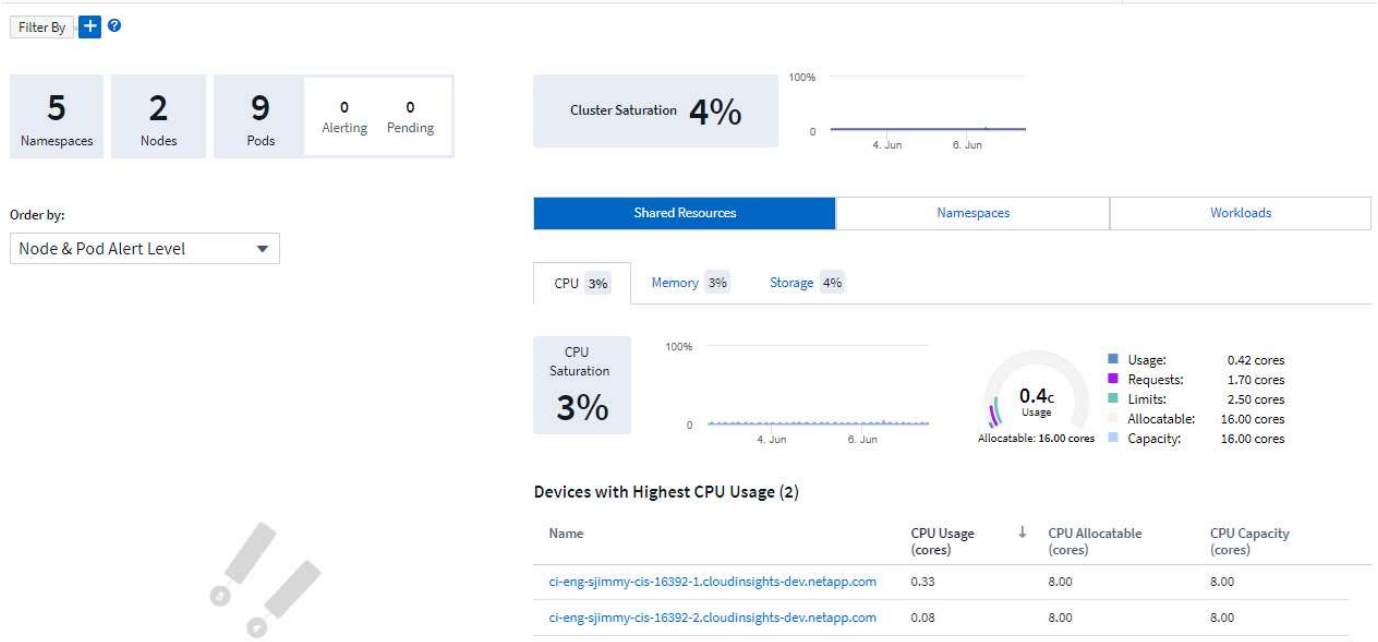
Oltre a quelli supportati da Cloud Insights Acquisition Units, è supportato anche il seguente sistema operativo"già supportato" :

- Windows 11

Giugno 2022

Saturazione del cluster Kubernetes e altri dettagli

Cloud Insights semplifica più che mai l'esplorazione dell'ambiente Kubernetes, con una pagina dei dettagli del cluster migliorata che fornisce dettagli sulla saturazione e una visualizzazione più chiara di spazi dei nomi e carichi di lavoro.

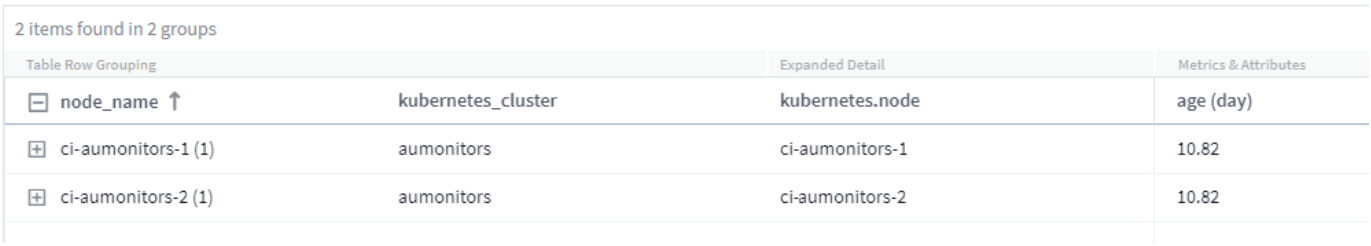


La pagina dell'elenco dei cluster fornisce anche una rapida panoramica della saturazione, oltre ai conteggi di

nodi, pod, spazi dei nomi e carichi di lavoro:

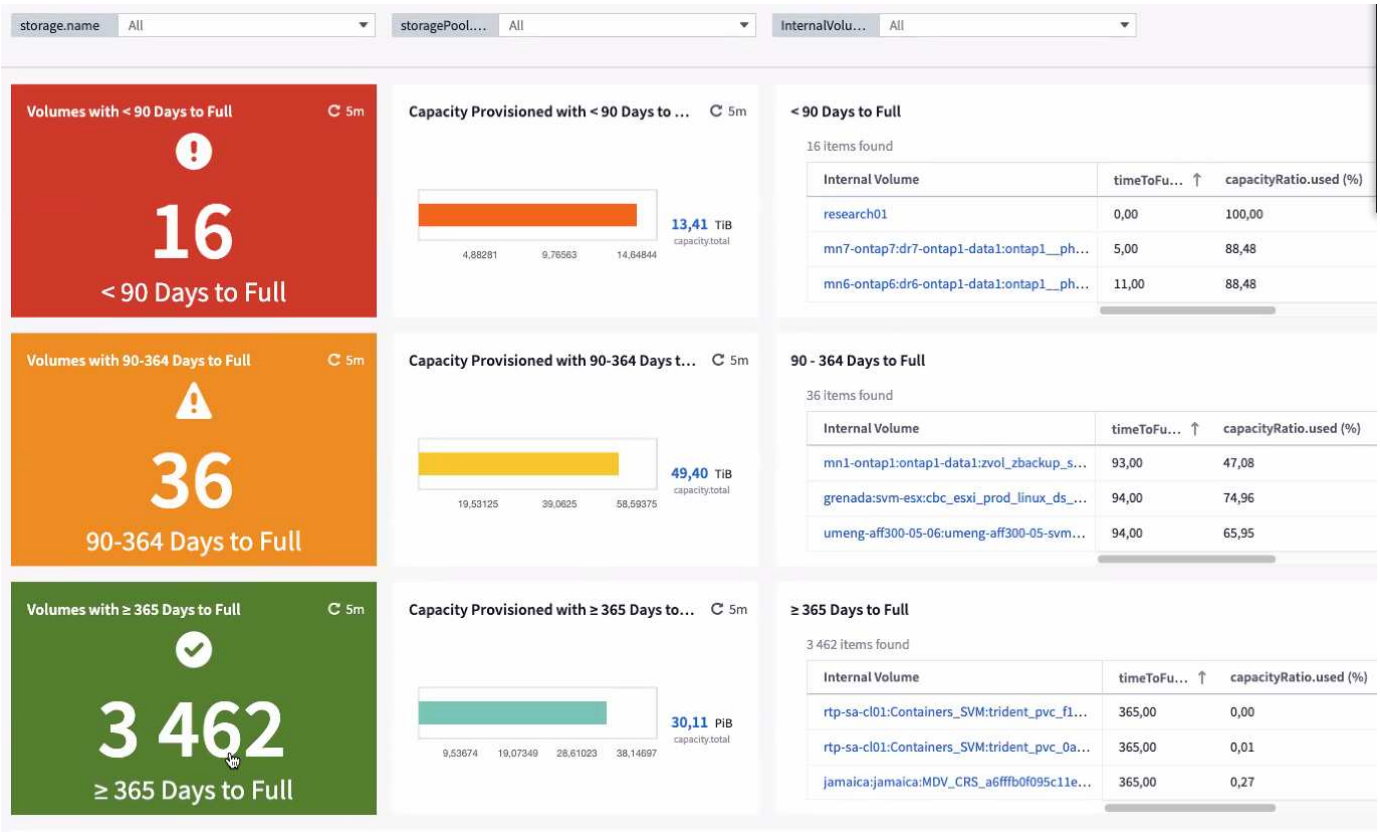
Quanti anni ha il tuo cluster Kubernetes?

Il tuo cluster è appena agli inizi o ha già una lunga storia digitale? *Age* è stato aggiunto come metrica temporale raccolta per i nodi Kubernetes.



Previsione del tempo di riempimento della capacità

Cloud Insights fornisce una dashboard per prevedere il numero di giorni che mancano all'esaurimento della capacità per ciascun volume interno monitorato. Questi valori possono contribuire a ridurre significativamente il rischio di interruzione.

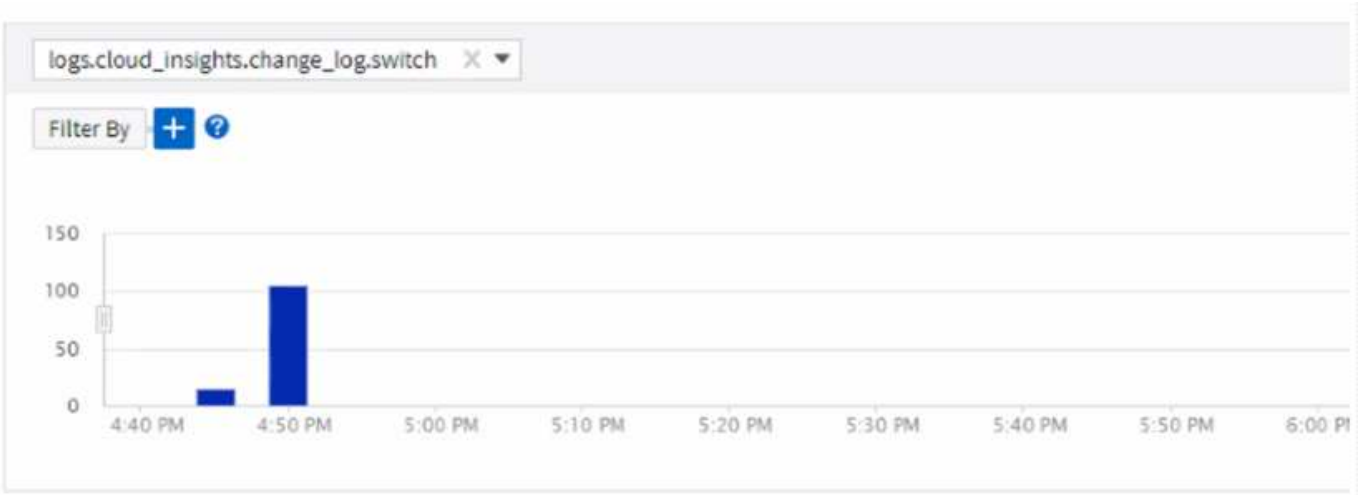


I contatori TTF sono disponibili anche per Storage, Storage Pool e Volume. Continuate a seguire questo spazio per ulteriori dashboard relative a questi oggetti.

Si noti che la previsione Time-to-Full non sarà più disponibile in *Anteprima* e verrà estesa a tutti i clienti.

Cosa è cambiato nel mio ambiente?

Le voci del registro delle modifiche ONTAP possono essere visualizzate nell'esploratore dei registri.



Log Entries

timestamp	name	object_type	message
06/08/2022 4:52:51 PM	fc19	Port	Port with name:fc19 has been created
06/08/2022 4:52:51 PM	fc20	Port	Port with name:fc20 has been created
06/08/2022 4:52:51 PM	fc23	Port	Port with name:fc23 has been created
06/08/2022 4:52:51 PM	fc22	Port	Port with name:fc22 has been created

Supporto del sistema operativo

Oltre a quelli supportati da Cloud Insights Acquisition Units, sono supportati anche i seguenti sistemi operativi:"già supportato" :

- CentOS Stream 9
- Windows 2022

Agente Telegraf aggiornato

L'agente per l'inserimento dei dati di integrazione Telegraf è stato aggiornato alla versione **1.22.3**, con miglioramenti delle prestazioni e della sicurezza. Gli utenti che desiderano effettuare l'aggiornamento possono fare riferimento alla sezione di aggiornamento appropriata del"Installazione dell'agente" documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza che sia richiesto alcun intervento da parte dell'utente.

Funzionalità di anteprima

Cloud Insights evidenzia regolarmente una serie di nuove interessanti funzionalità di anteprima. Se sei interessato a visualizzare in anteprima una o più di queste funzionalità, contatta il tuo"Team di vendita NetApp" per maggiori informazioni.

Caratteristica	Descrizione
Gli spazi dei nomi di Kubernetes stanno esaurendo lo spazio	L'Insight *Kubernetes Namespaces Running Out of Space* fornisce una panoramica dei carichi di lavoro sui namespace Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si riempia."Per saperne di più"
Cloud Secure : blocca l'accesso degli utenti in caso di attacco	Maggiore protezione per i dati aziendali critici con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando i criteri di risposta automatica, oppure manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Per saperne di più"
Risorsa condivisa sotto stress	L'insight *Shared Resource Under Stress* utilizza l'intelligenza artificiale e l'apprendimento automatico per identificare automaticamente dove la contesa delle risorse sta causando un degrado delle prestazioni nel tuo ambiente, evidenzia tutti i carichi di lavoro interessati e fornisce azioni consigliate per porvi rimedio, consentendoti di risolvere i problemi di prestazioni più rapidamente."Per saperne di più"

Maggio 2022

Chatta in diretta con il supporto NetApp

Ora puoi chattare in diretta con il personale di supporto NetApp ! Nella pagina Aiuto > Supporto, fai clic sull'icona Chat o su *Chat* nella sezione "Contattaci" per avviare una sessione di chat. L'assistenza tramite chat è disponibile nei giorni feriali negli Stati Uniti per gli utenti delle edizioni Standard e Premium.

Operatore Kubernetes

Abbiamo semplificato l'avvio del tuo progetto con il monitoraggio avanzato di Kubernetes e l'esploratore di cluster Cloud Insights.

IL"Operatore di monitoraggio Kubernetes" (NKMO) è il metodo preferito per installare Kubernetes per Cloud

Insights Insights, per una configurazione più flessibile del monitoraggio in meno passaggi, nonché maggiori opportunità di monitoraggio di altri software in esecuzione nel cluster K8s.

Clicca sul link sopra per maggiori informazioni e prerequisiti

Gestisci utenti e inviti con API

Ora puoi gestire utenti e inviti utilizzando la potente API di Cloud Insights. Leggi di più nel"Documentazione API Swagger" .

Avvisi sulla raccolta dati

Non perdere metriche critiche a causa di un collettore non riuscito!

È più facile che mai tenere traccia dei tuoi raccoglitori di dati con il nuovo"avvisi" per guasti al raccoglitore dati e all'unità di acquisizione. Si noti che questi monitor sono *in pausa* per impostazione predefinita. Per abilitare, vai alla pagina dei tuoi monitor e individua e riprendi "Acquisition Unit Shutdown" e "Collector Failed"

Avviso sulle modifiche allo storage ONTAP

Non lasciare che cambiamenti inaspettati nello storage provochino interruzioni!

Ora puoi configurare Cloud Insights per ricevere un avviso quando vengono rilevate modifiche o rimozioni di FlexVol, nodi e SVM sui sistemi ONTAP .

Funzionalità di anteprima

Cloud Insights evidenzia regolarmente una serie di nuove interessanti funzionalità di anteprima. Se sei interessato a visualizzare in anteprima una o più di queste funzionalità, contatta il tuo"Team di vendita NetApp" per maggiori informazioni.

Caratteristica	Descrizione
Gli spazi dei nomi di Kubernetes stanno esaurendo lo spazio	L'Insight *Kubernetes Namespaces Running Out of Space* fornisce una panoramica dei carichi di lavoro sui namespace Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si riempia."Per saperne di più"
Previsione del tempo di riempimento del volume interno e della capacità di volume	Cloud Insights è in grado di prevedere il numero di giorni che mancano all'esaurimento della capacità per ciascun volume interno e volume monitorato. Questo valore può contribuire a ridurre significativamente il rischio di interruzione.
Cloud Secure : blocca l'accesso degli utenti in caso di attacco	Maggiore protezione per i dati aziendali critici con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando i criteri di risposta automatica, oppure manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Per saperne di più"

Risorsa condivisa sotto stress	L'insight *Shared Resource Under Stress* utilizza l'intelligenza artificiale e l'apprendimento automatico per identificare automaticamente dove la contesa delle risorse sta causando un degrado delle prestazioni nel tuo ambiente, evidenzia tutti i carichi di lavoro interessati e fornisce azioni consigliate per porvi rimedio, consentendoti di risolvere i problemi di prestazioni più rapidamente."Per saperne di più"

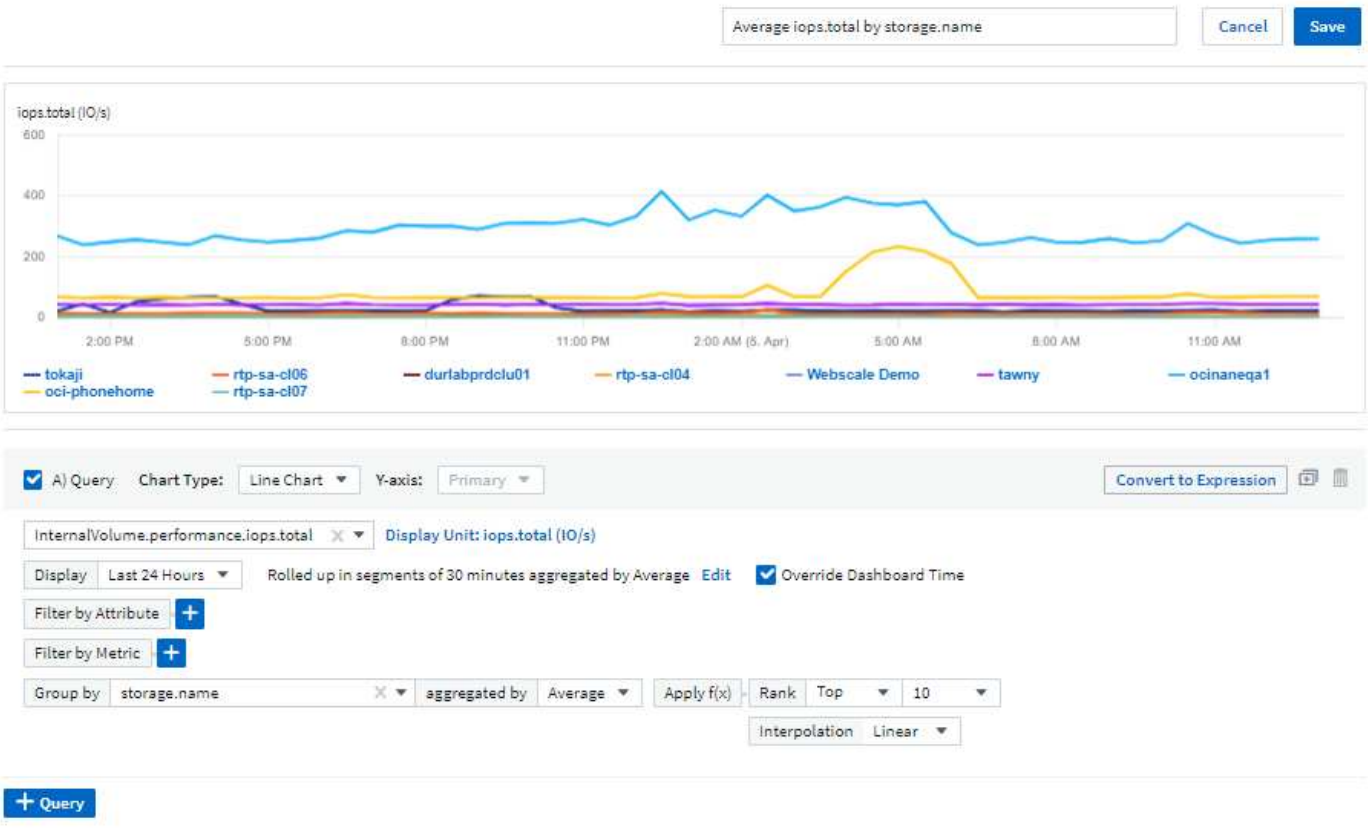
Aprile 2022

Condividi il tuo feedback!

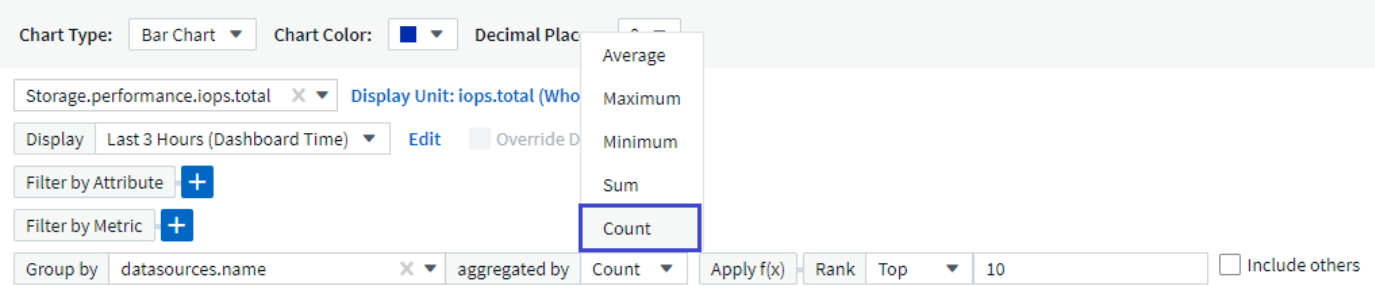
Vogliamo il tuo contributo per aiutarci a dare forma a Cloud Insights. Guadagna punti e premi partecipando al programma **Insights to Action** di NetApp. **"Iscriviti ora"** !

Dashboard Editor aggiornato

Abbiamo rivisto i nostri strumenti di creazione della dashboard per consentirti di visualizzare i tuoi dati ancora più facilmente e rapidamente. Vai alla pagina "Dashboard" di Cloud Insights per modificare una dashboard esistente, aggiungerne una dalla nostra galleria di dashboard o crearne una nuova per verificarla.



È stato introdotto anche un nuovo metodo di aggregazione dei conteggi. Quando si raggruppano i dati nei widget grafico a barre, grafico a colonne e grafico a torta, è possibile visualizzare in modo semplice e rapido il numero di oggetti rilevanti per la metrica selezionata.



Inoltre, i grafici a linee ora consentono di selezionare uno dei tre"interpolazione" metodi:

- Nessuno - Non viene eseguita alcuna interpolazione
- Lineare - Interpola un punto dati tra i punti esistenti
- Scala: utilizza il punto dati precedente come punto dati interpolato

Monitoraggio avanzato per la tua infrastruttura Kubernetes

Cloud Insights ti tiene aggiornato sulle modifiche apportate al tuo ambiente Kubernetes avvisandoti quando vengono creati o rimossi pod, daemonset e replicaset, nonché quando vengono create nuove distribuzioni. Per impostazione predefinita, i monitor Kubernetes sono in stato *paused*, quindi dovresti abilitare solo quelli specifici di cui hai bisogno.

Funzionalità di anteprima

Cloud Insights evidenzia regolarmente una serie di nuove interessanti funzionalità di anteprima. Se sei interessato a visualizzare in anteprima una o più di queste funzionalità, contatta il tuo"Team di vendita NetApp" per maggiori informazioni.

Caratteristica	Descrizione
Previsione del tempo di riempimento del volume interno e della capacità di volume	Cloud Insights è in grado di prevedere il numero di giorni che mancano all'esaurimento della capacità per ciascun volume interno e volume monitorato. Questo valore può contribuire a ridurre significativamente il rischio di interruzione.
Cloud Secure : blocca l'accesso degli utenti in caso di attacco	Maggiore protezione per i dati aziendali critici con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando i criteri di risposta automatica, oppure manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Per saperne di più"
Risorsa condivisa sotto stress	L'insight Shared Resource Under Stress utilizza l'intelligenza artificiale e l'apprendimento automatico per identificare automaticamente dove la contesa delle risorse sta causando un degrado delle prestazioni nel tuo ambiente, evidenzia eventuali carichi di lavoro interessati e fornisce azioni consigliate per porvi rimedio, consentendoti di risolvere i problemi di prestazioni più rapidamente."Per saperne di più"

Nuovo raccoglitore di dati

- **Cohesity SmartFiles** - Questo raccoglitore basato su API REST acquisirà un cluster Cohesity, scoprendo le "Visualizzazioni" (come volumi interni CI), i vari nodi e raccogliendo metriche sulle prestazioni.

Altri aggiornamenti del Data Collector

La raccolta e la visualizzazione dei dati sulle prestazioni sono state migliorate sui seguenti collettori di dati:

- Interfaccia a riga di comando Brocade
- Dell/EMC VPlex, PowerStore, Isilon/PowerScale, VNX Block/Clariion CLI, XtremIO, Unity/VNXe
- FlashArray puro

Questi miglioramenti delle prestazioni sono già disponibili in tutti i data collector NetApp , nonché in VMware e Cisco, e saranno estesi a tutti gli altri data collector nei prossimi mesi.

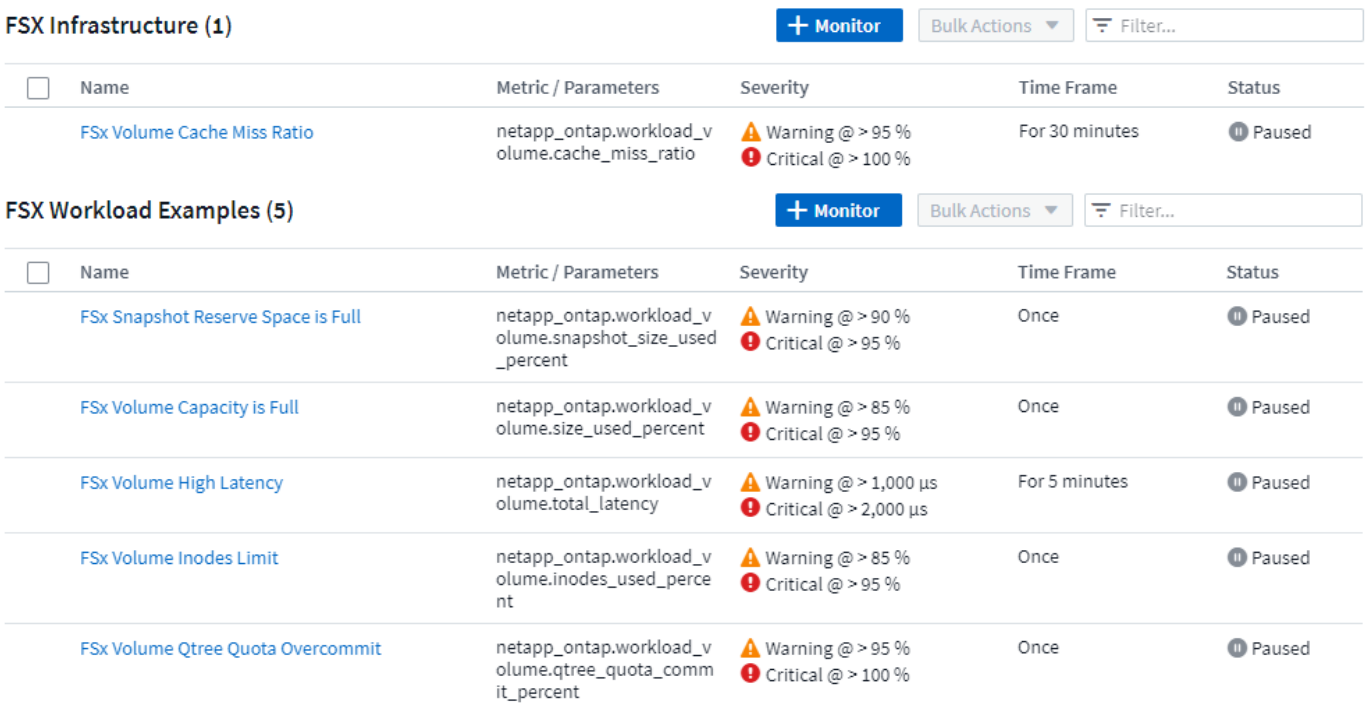
Marzo 2022

Connessione cloud per ONTAP 9.9+

IL"Connessione NetApp Cloud per ONTAP 9.9+" Il raccoglitore di dati elimina la necessità di installare un'unità di acquisizione esterna, semplificando così la risoluzione dei problemi, la manutenzione e l'implementazione iniziale.

Nuovo FSx per i monitor NetApp ONTAP

Il monitoraggio del tuo ambiente FSx per NetApp ONTAP è facile con il nuovo"monitor definiti dal sistema" sia per l'infrastruttura (metriche) che per i carichi di lavoro (registri).



Nuove funzionalità Cloud Secure disponibili per tutti

Il tuo ambiente è più sicuro che mai con le seguenti funzionalità Cloud Secure ora disponibili al pubblico:

Caratteristica	Descrizione
Distruzione dei dati – Rilevamento degli attacchi di eliminazione dei file	Rileva attività di eliminazione di file anomale su larga scala, blocca l'accesso dannoso ai file da parte di utenti malintenzionati ed esegui snapshot automatici con criteri di risposta automatica.
Notifiche separate per avvisi e avvisi	Le notifiche di avviso e di allerta possono essere inviate a destinatari separati, garantendo che il team giusto possa rimanere informato

Agente Telegraf aggiornato

L'agente per l'inserimento dei dati di integrazione Telegraf è stato aggiornato alla versione **1.21.2**, con miglioramenti delle prestazioni e della sicurezza. Gli utenti che desiderano effettuare l'aggiornamento possono fare riferimento alla sezione di aggiornamento appropriata del"Installazione dell'agente" documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza che sia richiesto alcun intervento da parte dell'utente.

Aggiornamenti del Data Collector

- Il raccoglitore dati degli switch Fibre Channel Broadcom è stato ottimizzato per ridurre il numero di comandi CLI emessi con ogni polling di inventario.

Febbraio 2022

Cloud Insights risolve le vulnerabilità di Apache Log4j

Per NetApp la sicurezza dei clienti è una priorità assoluta. Cloud Insights include aggiornamenti alle sue librerie software per risolvere le recenti vulnerabilità di Apache Log4j.

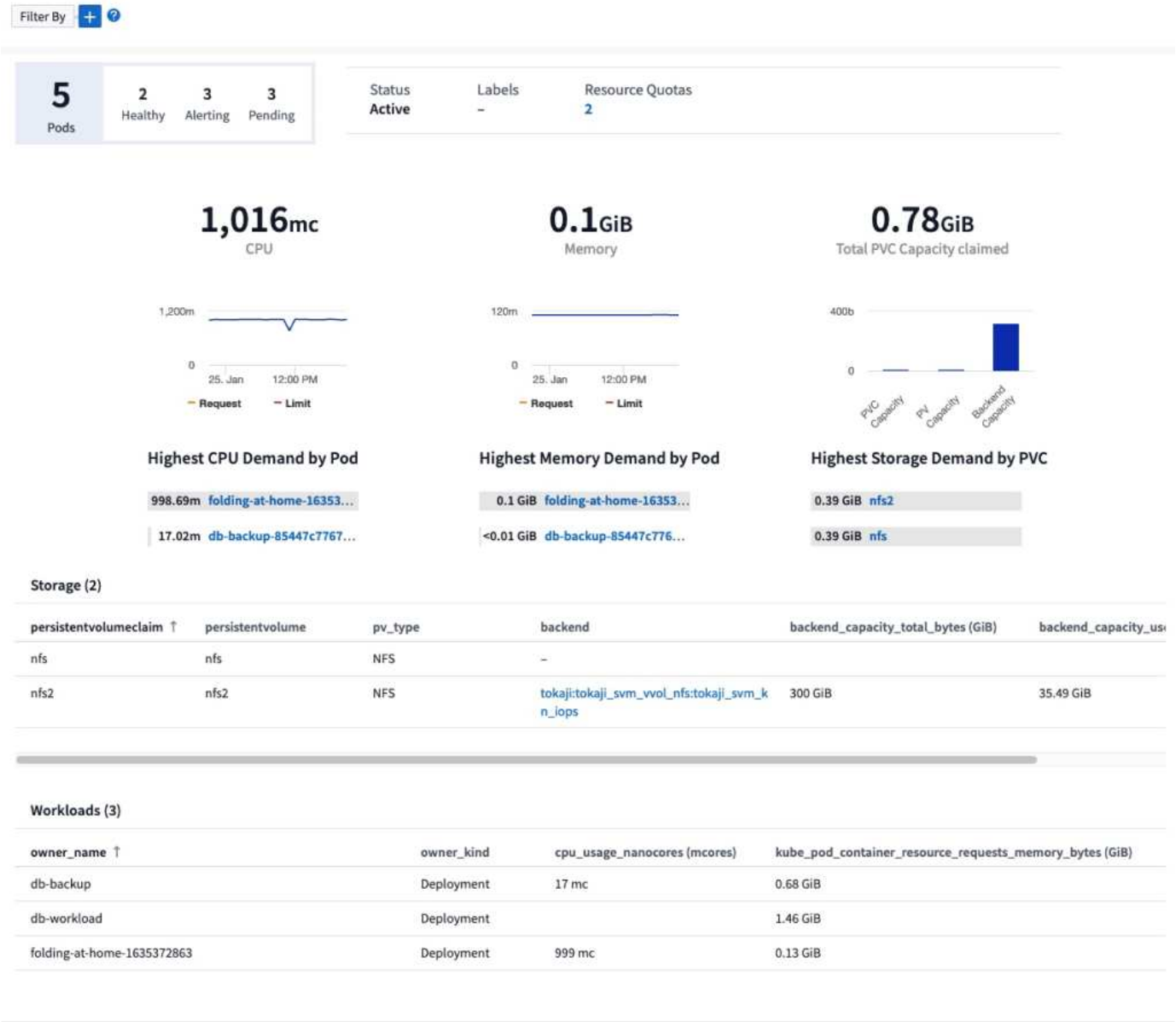
Fare riferimento a quanto segue sul sito Web Product Security Advisory di NetApp:

"CVE-2021-44228" "CVE-2021-45046" "CVE-2021-45105"

Puoi leggere di più su queste vulnerabilità e sulla risposta di NetApp su"Sala stampa NetApp" .

Pagina dei dettagli dello spazio dei nomi Kubernetes

Esplorare il tuo ambiente Kubernetes è ora più semplice che mai, grazie alle pagine dettagliate e informative sugli spazi dei nomi del tuo cluster. La pagina dei dettagli dello spazio dei nomi fornisce un riepilogo di tutte le risorse utilizzate da uno spazio dei nomi, comprese tutte le risorse di archiviazione back-end e il loro utilizzo della capacità.



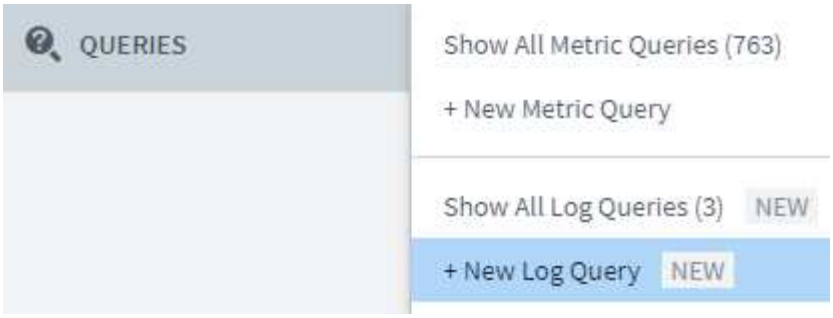
Dicembre 2021

Integrazione più profonda per i sistemi ONTAP

Semplifica gli avvisi per guasti hardware ONTAP e altro ancora con la nuova integrazione con NetApp Event Management System (EMS). "Esplora e avvisa" sui messaggi ONTAP di basso livello in Cloud Insights per informare e migliorare i flussi di lavoro di risoluzione dei problemi e ridurre ulteriormente la dipendenza dagli strumenti di gestione degli elementi ONTAP .

Interrogazione dei registri

Per i sistemi ONTAP , le query Cloud Insights includono un potente"Esploratore di log" , consentendo di analizzare e risolvere facilmente i problemi delle voci del registro EMS.



Notifiche a livello di Data Collector.

Oltre ai monitor definiti dal sistema e creati su misura per gli avvisi, è anche possibile impostare notifiche di avviso per i raccoglitori di dati ONTAP , consentendo di specificare i destinatari per gli avvisi a livello di raccoglitore, indipendentemente dagli altri avvisi del monitor.

Maggiore flessibilità dei ruoli Cloud Secure

Agli utenti può essere concesso l'accesso alle funzionalità Cloud Secure in base a"ruoli" impostato da un amministratore:

Ruolo	Accesso Cloud Secure
Amministratore	Può eseguire tutte le funzioni Cloud Secure , comprese quelle per avvisi, analisi forense, raccoglitori di dati, policy di risposta automatizzate e API per Cloud Secure. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli Cloud Secure .
Utente	Può visualizzare e gestire gli avvisi e visualizzare le analisi forensi. Il ruolo utente può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot e bloccare l'accesso utente.
Ospite	È possibile visualizzare avvisi e analisi forensi. Il ruolo ospite non può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot o bloccare l'accesso utente.

Supporto del sistema operativo

Il supporto CentOS 8.x verrà sostituito dal supporto **CentOS 8 Stream**. CentOS 8.x raggiungerà la fine del suo ciclo di vita il 31 dicembre 2021.

Aggiornamenti del Data Collector

Sono stati aggiunti diversi nomi di raccoglitori di dati Cloud Insights per riflettere le modifiche apportate dal fornitore:

Fornitore/Modello	Nome precedente
Dell EMC PowerScale	Isilon

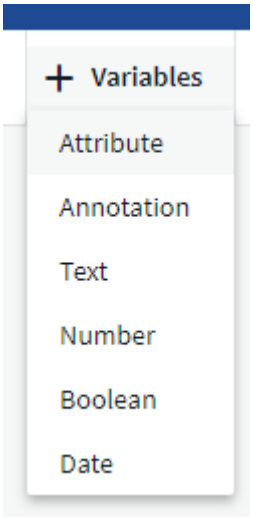
HPE Alletra 9000 / Primera	3PAR
HPE Alletra 6000	Agile

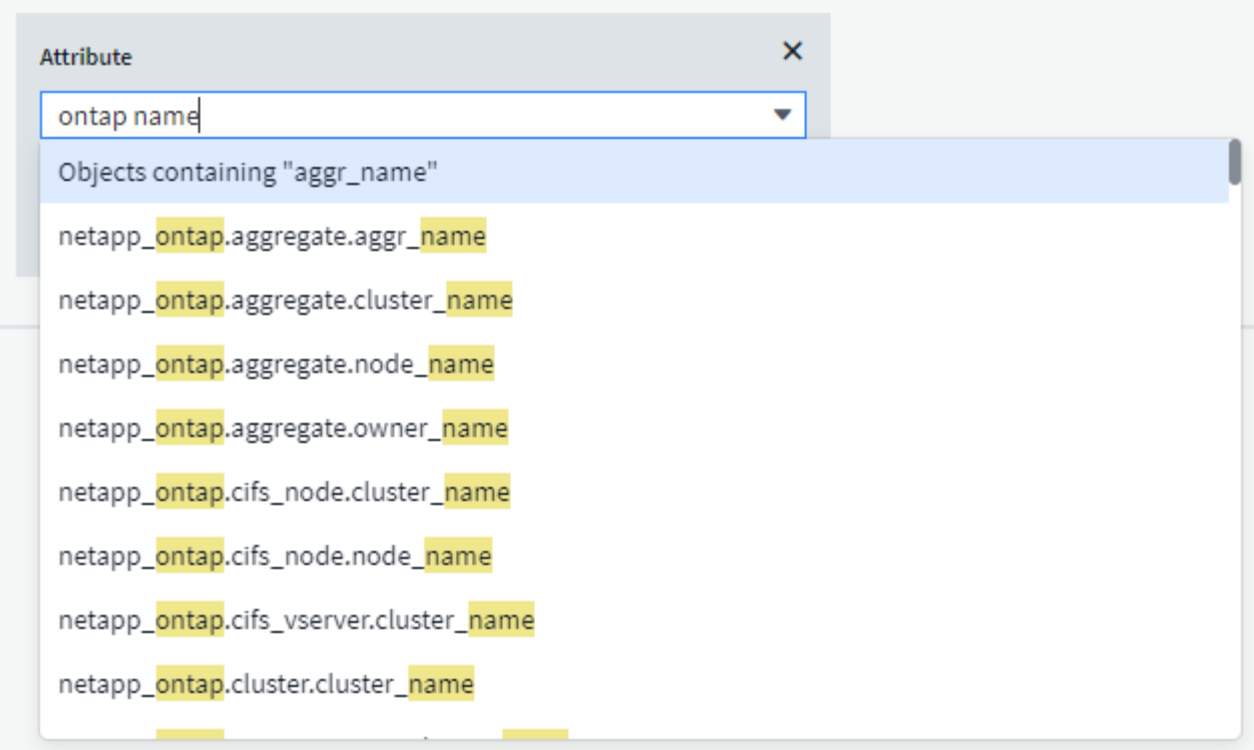
Novembre 2021

Dashboard adattive

Nuove variabili per gli attributi e possibilità di utilizzare variabili nei widget.

Le dashboard sono ora più potenti e flessibili che mai. Crea dashboard adattive con variabili di attributo per filtrare rapidamente le dashboard al volo. Utilizzando questi e altri preesistenti"variabili" Ora puoi creare una dashboard di alto livello per visualizzare le metriche dell'intero ambiente e filtrarle senza problemi in base al nome della risorsa, al tipo, alla posizione e altro ancora. Utilizzare variabili numeriche nei widget per associare metriche grezze ai costi, ad esempio il costo per GB per l'archiviazione come servizio.





Accedi al database di reporting tramite API

Funzionalità avanzate per l'integrazione con strumenti di reporting, ITSM e automazione di terze parti: la potente tecnologia Cloud Insights"API" consente agli utenti di interrogare direttamente il database di Cloud Insights Reporting, senza passare attraverso l'ambiente di Cognos Reporting.

Tabelle pod nella landing page della VM

Navigazione fluida tra le VM e i Kubernetes Pod che le utilizzano: per una migliore risoluzione dei problemi e gestione del margine di prestazioni, ora nelle landing page delle VM verrà visualizzata una tabella dei Kubernetes Pod associati.

Aggiornamenti del Data Collector

- ECS ora segnala il firmware per l'archiviazione e il nodo
- Isilon ha migliorato il rilevamento rapido
- Azure NetApp Files raccoglie i dati sulle prestazioni più rapidamente
- StorageGRID ora supporta Single Sign-On (SSO)
- Brocade CLI segnala correttamente il modello per X&-4

Sistemi operativi aggiuntivi supportati

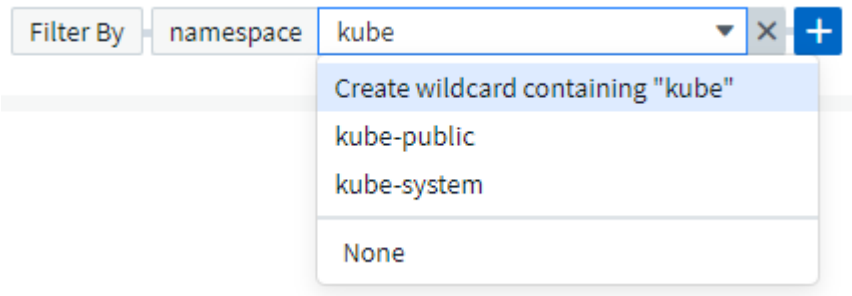
Oltre a quelli già supportati, Cloud Insights Acquisition Unit supporta i seguenti sistemi operativi:

- Centos (64 bit) 8.4
- Oracle Enterprise Linux (64 bit) 8.4
- Red Hat Enterprise Linux (64 bit) 8.4

Ottobre 2021

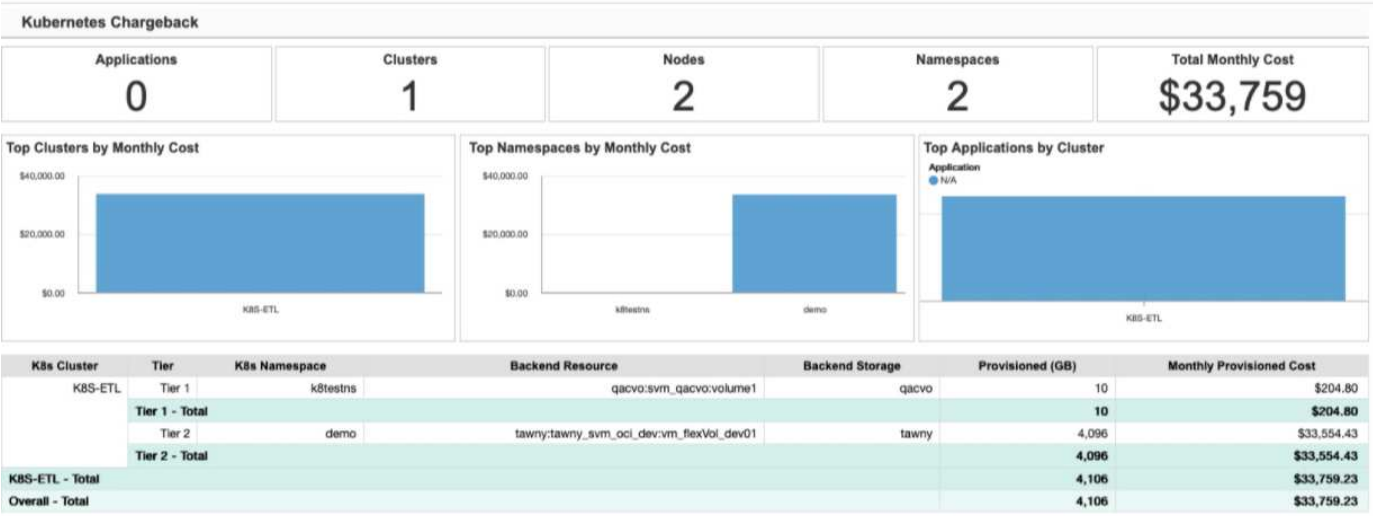
Filtri sulle pagine di K8S Explorer

"Esploratore Kubernetes"I filtri di pagina ti offrono un controllo mirato sui dati visualizzati per l'esplorazione di cluster, nodi e pod Kubernetes.



Dati K8s per la segnalazione

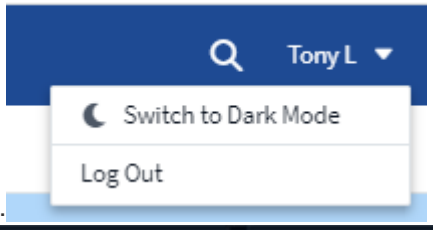
I dati di Kubernetes sono ora disponibili per l'utilizzo in Reporting, consentendo di creare report di addebito o di altro tipo. Affinché i dati di addebito di Kubernetes vengano trasmessi a Reporting, è necessario disporre di una connessione attiva al cluster Kubernetes e al suo storage back-end, e Cloud Insights deve ricevere dati da esso. Se non vengono ricevuti dati dall'archiviazione back-end, Cloud Insights non può inviare dati sugli oggetti Kubernetes a Reporting.

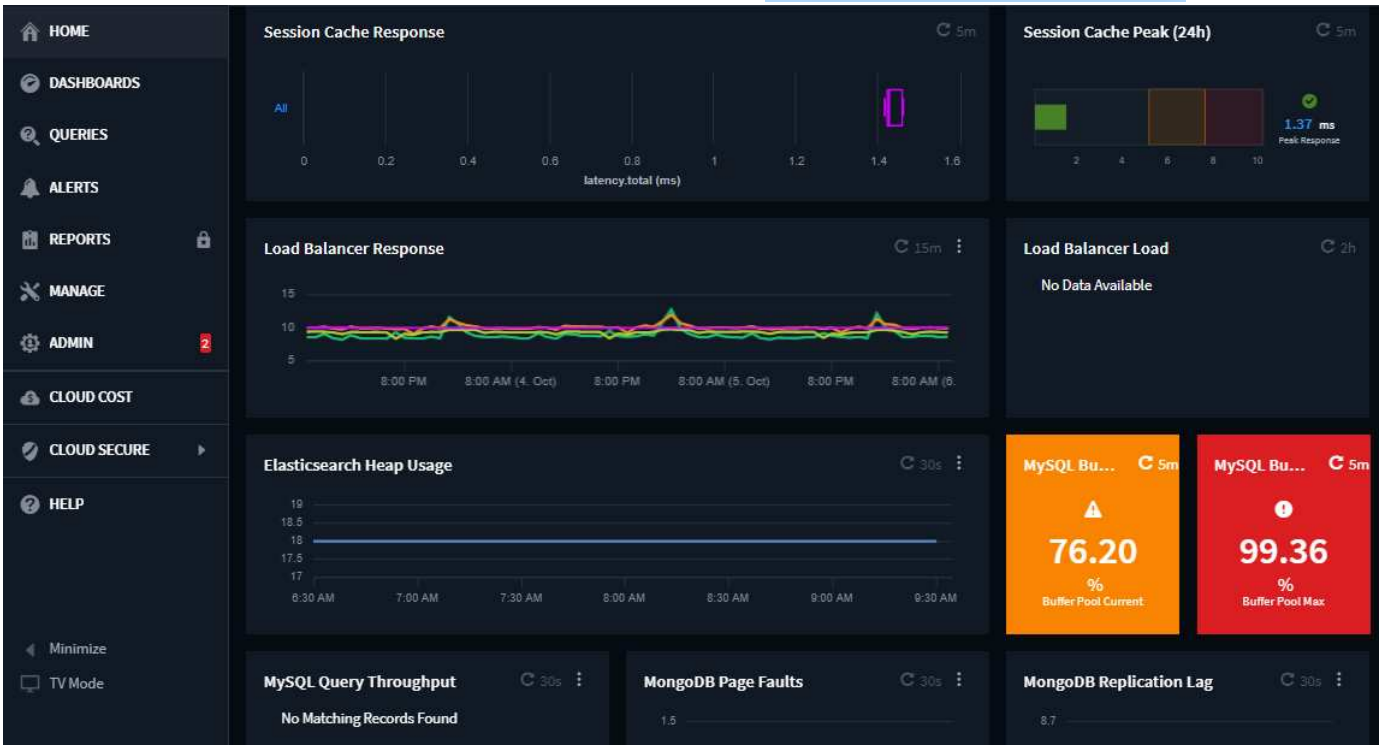


K8s Cluster	Tier	K8s Namespace	Backend Resource	Backend Storage	Provisioned (GB)	Monthly Provisioned Cost
K8S-ETL	Tier 1	k8testns	qacvo:svm_qacvo:volume1	qacvo	10	$204.80
	Tier 1 - Total				**10**	**$204.80**
	Tier 2	demo	tawny:tawny_svm_oci_dev:vm_flexVol_dev01	tawny	4,096	$33,554.43
	Tier 2 - Total				**4,096**	**$33,554.43**
K8S-ETL - Total					**4,106**	**$33,759.23**
Overall - Total					**4,106**	**$33,759.23**

È arrivato il tema scuro

Molti di voi hanno chiesto un tema scuro e Cloud Insights ha risposto. Per passare dal tema chiaro a quello scuro, fai clic sul menu a discesa accanto al tuo nome utente.





Supporto per la raccolta dati

Abbiamo apportato alcuni miglioramenti a Cloud Insights Data Collectors. Ecco alcuni punti salienti:

- Nuovo collettore per Amazon FSx per ONTAP

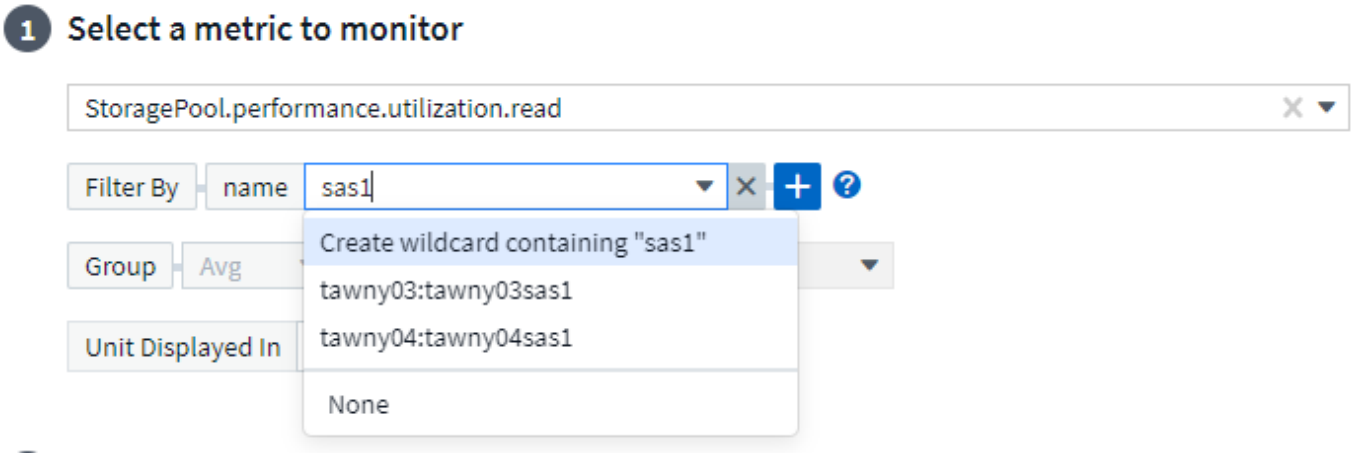
Settembre 2021

Le policy sulle prestazioni ora sono monitor

Monitor e avvisi hanno sostituito i criteri e le violazioni delle prestazioni in Cloud Insights. "Avvisi con monitor" offre maggiore flessibilità e approfondimenti su potenziali problemi o tendenze nel tuo ambiente.

Suggerimenti di completamento automatico, caratteri jolly ed espressioni nei monitor

Quando si crea un monitor per gli avvisi, l'inserimento di un filtro è ora predittivo, consentendo di cercare e trovare facilmente le metriche o gli attributi per il monitor. Inoltre, ti viene data la possibilità di creare un filtro con caratteri jolly in base al testo digitato.



Agente Telegraf aggiornato

L'agente per l'inserimento dei dati di integrazione Telegraf è stato aggiornato alla versione **1.19.3**, con miglioramenti delle prestazioni e della sicurezza. Gli utenti che desiderano effettuare l'aggiornamento possono fare riferimento alla sezione di aggiornamento appropriata del"Installazione dell'agente" documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza che sia richiesto alcun intervento da parte dell'utente.

Supporto per la raccolta dati

Abbiamo apportato alcuni miglioramenti a Cloud Insights Data Collectors. Ecco alcuni punti salienti:

- Microsoft Hyper-V Collector ora utilizza PowerShell anziché WMI
- Le macchine virtuali di Azure e il raccoglitore VHD sono ora fino a 10 volte più veloci grazie alle chiamate parallele
- HPE Nimble ora supporta configurazioni federate e iSCSI

E poiché stiamo costantemente migliorando la raccolta dati, ecco alcune altre recenti modifiche degne di nota:

- Nuovo collettore per EMC Powerstore
- Nuovo collettore per Hitachi Ops Center
- Nuovo collettore per Hitachi Content Platform
- Collettore ONTAP migliorato per segnalare i Fabric Pool
- ANF migliorato con prestazioni di volume e pool di archiviazione
- EMC ECS migliorato con nodi di archiviazione e prestazioni di archiviazione, nonché conteggio degli oggetti nei bucket
- EMC Isilon migliorato con metriche Storage Node e Qtree
- EMC Symetrix migliorato con metriche di limite QOS del volume
- Numero di serie padre di IBM SVC ed EMC PowerStore con Storage Nodes migliorato

Agosto 2021

Nuova interfaccia utente della pagina di controllo

IL"Pagina di controllo" fornisce un'interfaccia più pulita e ora consente l'esportazione degli eventi di audit in un file .CSV.

Gestione avanzata dei ruoli utente

Cloud Insights ora consente ancora più libertà nell'assegnazione dei ruoli utente e nei controlli di accesso. Ora agli utenti possono essere assegnate autorizzazioni granulari per il monitoraggio, la creazione di report e Cloud Secure separatamente.

Ciò significa che puoi consentire a più utenti l'accesso amministrativo alle funzioni di monitoraggio, ottimizzazione e reporting, limitando al contempo l'accesso ai dati sensibili di audit e attività Cloud Secure solo a coloro che ne hanno bisogno.

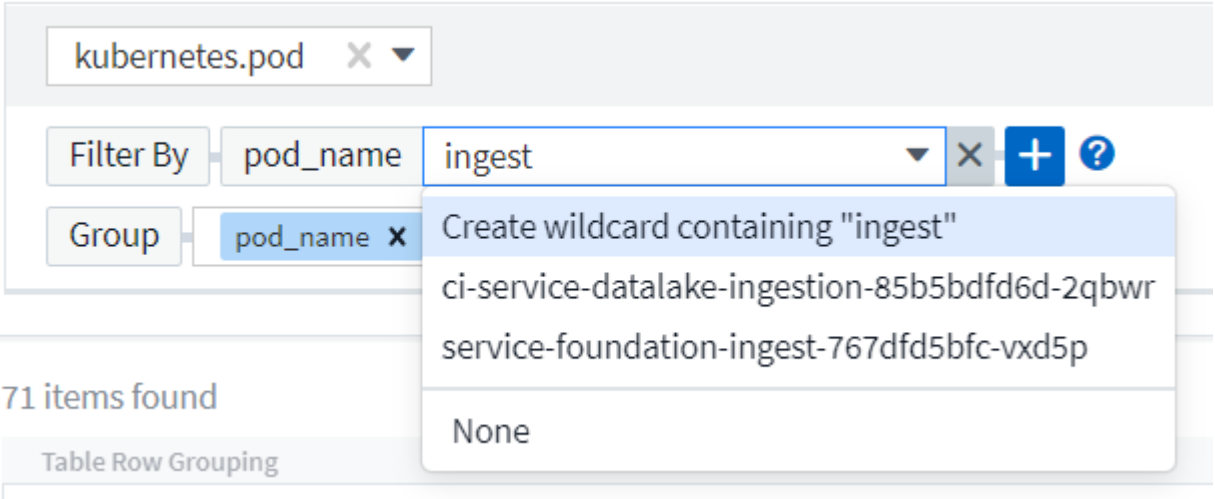
"Scopri di più"sui diversi livelli di accesso nella documentazione Cloud Insights .

Giugno 2021

Suggerimenti di completamento automatico, caratteri jolly ed espressioni nei filtri

Con questa versione di Cloud Insights, non è più necessario conoscere tutti i possibili nomi e valori in base ai quali filtrare una query o un widget. Quando si filtra, è sufficiente iniziare a digitare e Cloud Insights suggerirà valori in base al testo. Non è più necessario cercare in anticipo i nomi delle applicazioni o gli attributi di Kubernetes solo per trovare quelli che vuoi mostrare nel tuo widget.

Mentre digiti un filtro, il filtro visualizza un elenco intelligente di risultati tra cui puoi scegliere, oltre all'opzione per creare un **filtro jolly** in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione jolly. Naturalmente puoi anche selezionare più valori singoli che vuoi aggiungere al filtro.



Inoltre, è possibile creare **espressioni** in un filtro utilizzando NOT o OR, oppure è possibile selezionare l'opzione "Nessuno" per filtrare i valori nulli nel campo.

Per saperne di più"opzioni di filtraggio" nelle query e nei widget.

API disponibili per edizione

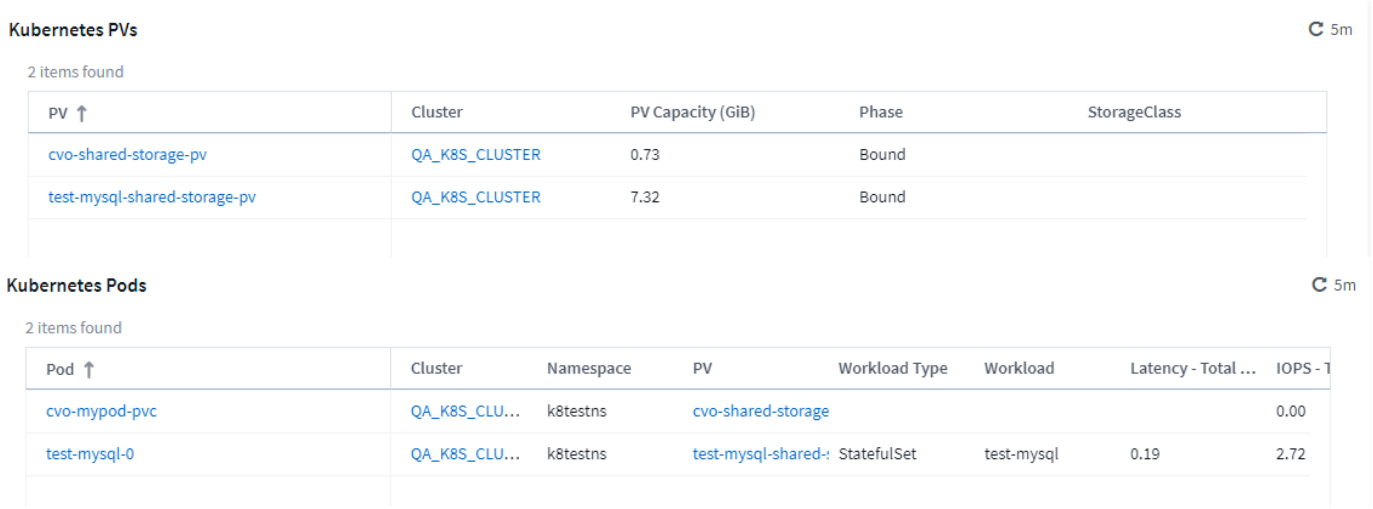
Le potenti API di Cloud Insights sono più accessibili che mai: le API Alerts sono ora disponibili nelle edizioni Standard e Premium. Per ogni edizione sono disponibili le seguenti API:

Categoria API	Di base	Standard	Premio
Unità di acquisizione	✔	✔	✔
Raccolta dati	✔	✔	✔
Avvisi		✔	✔
Attività		✔	✔
Inserimento dati		✔	✔

Visibilità di Kubernetes PV e Pod

Cloud Insights fornisce visibilità sullo storage back-end per i tuoi ambienti Kubernetes, fornendoti informazioni dettagliate sui tuoi Kubernetes Pod e Persistent Volumes (PV). Ora è possibile monitorare i contatori PV, come IOPS, latenza e throughput, dall'utilizzo di un singolo Pod tramite un contatore PV a un PV e fino al dispositivo di archiviazione back-end.

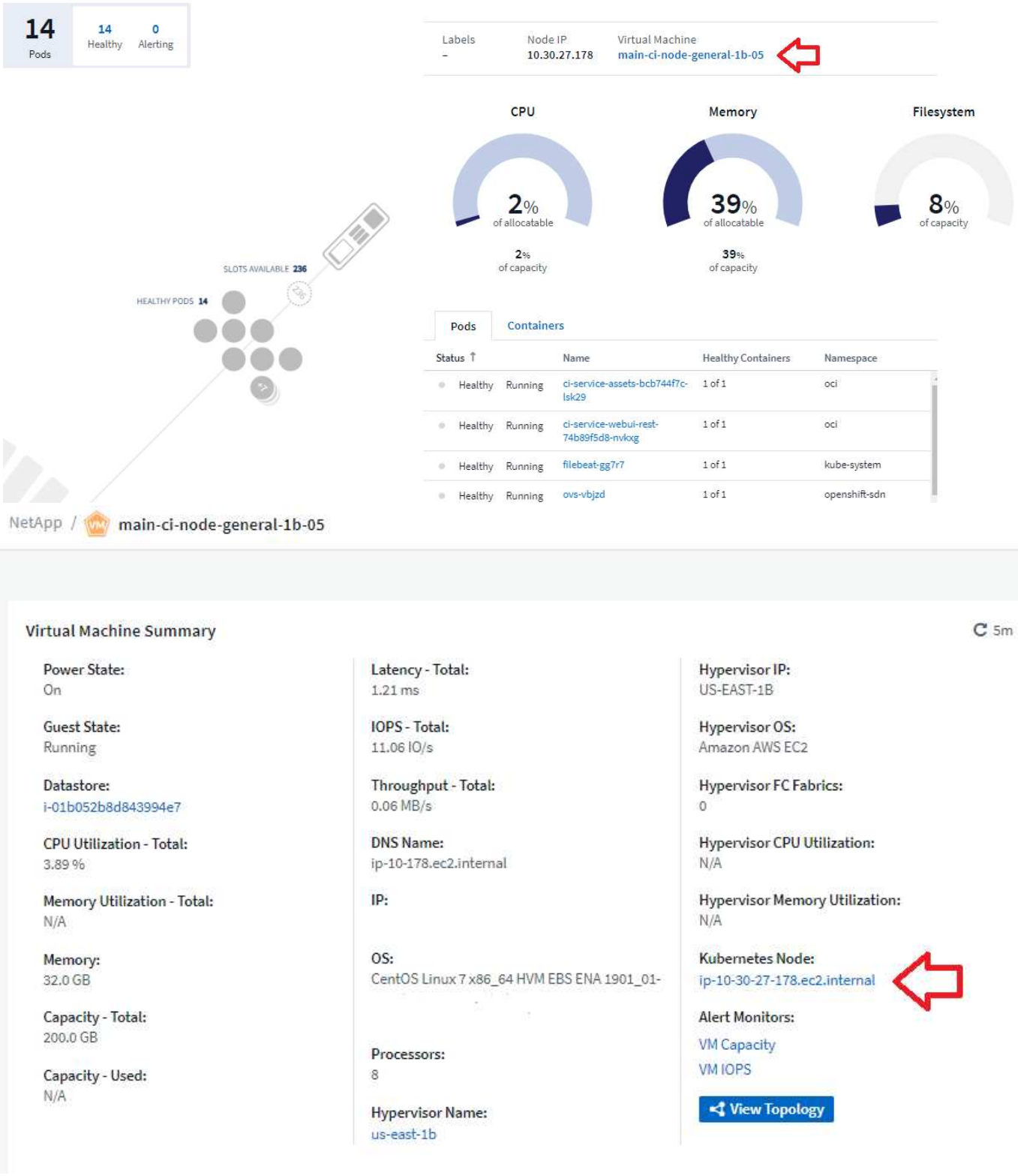
Nella landing page di un Volume o di un Volume interno vengono visualizzate due nuove tabelle:



Tieni presente che per sfruttare queste nuove tabelle, è consigliabile disinstallare l'agente Kubernetes corrente e installarne uno nuovo. È inoltre necessario installare Kube-State-Metrics versione 2.1.0 o successiva.

Collegamenti tra nodi Kubernetes e VM

Nella pagina di un nodo Kubernetes, ora puoi fare clic per aprire la pagina della VM del nodo. La pagina VM include anche un collegamento al Nodo stesso.



Monitor di avviso che sostituiscono i criteri di prestazione

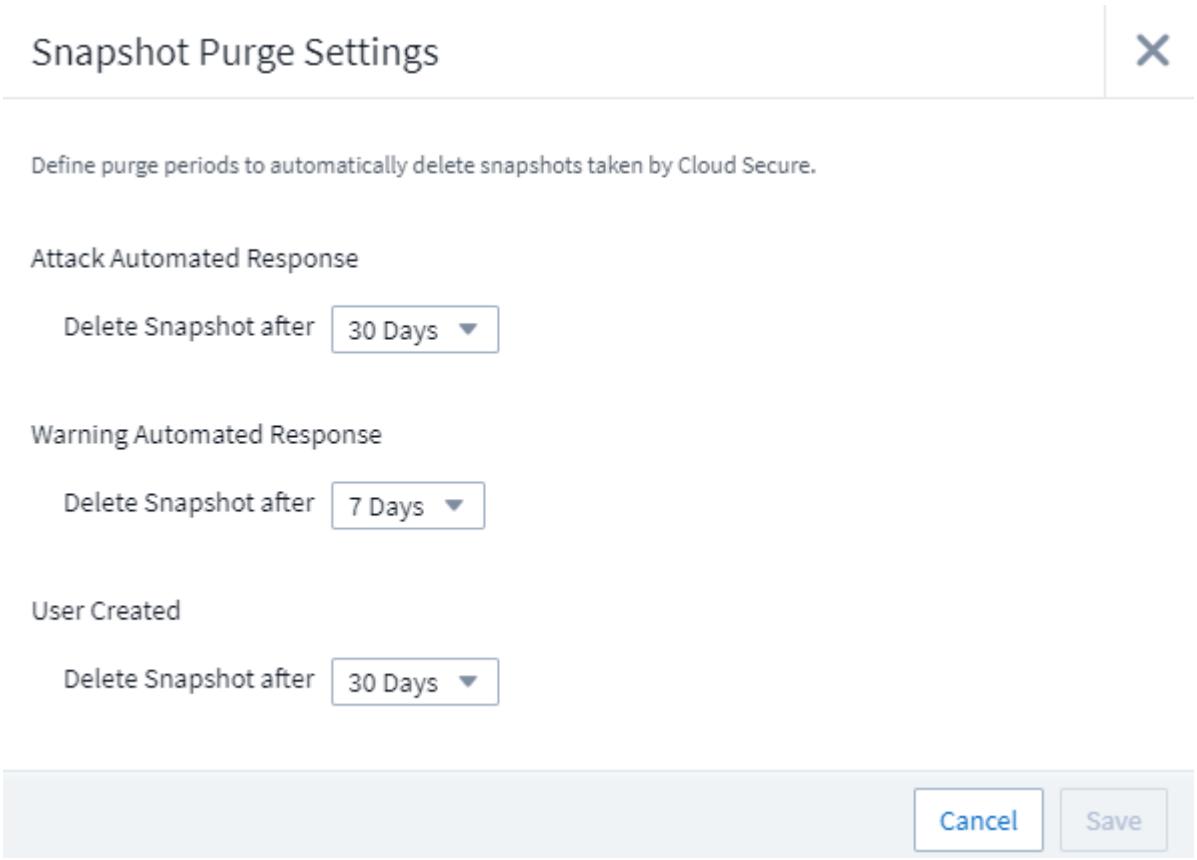
Per consentire i vantaggi aggiuntivi di soglie multiple, webhook e invio di avvisi via e-mail, avvisi su tutte le metriche tramite un'unica interfaccia e altro ancora, Cloud Insights convertirà i clienti della Standard e Premium Edition da **Performance Policies** a **Monitor** durante i mesi di luglio e agosto 2021. Scopri di più su"Avvisi e monitoraggi" e restate sintonizzati per scoprire questo entusiasmante cambiamento.

Cloud Secure supporta NFS

Cloud Secure ora supporta NFS per la raccolta dati ONTAP . Monitora l'accesso degli utenti SMB e NFS per proteggere i tuoi dati dagli attacchi ransomware. Inoltre, Cloud Secure supporta le directory utente Active Directory e LDAP per la raccolta degli attributi utente NFS.

Eliminazione Cloud Secure

Cloud Secure elimina automaticamente gli snapshot in base alle impostazioni di eliminazione degli snapshot, per risparmiare spazio di archiviazione e ridurre la necessità di eliminarli manualmente.



Velocità di raccolta dati Cloud Secure

Un singolo sistema di raccolta dati può ora pubblicare fino a 20.000 eventi al secondo su Cloud Secure.

Maggio 2021

Ecco alcune delle modifiche apportate ad aprile:

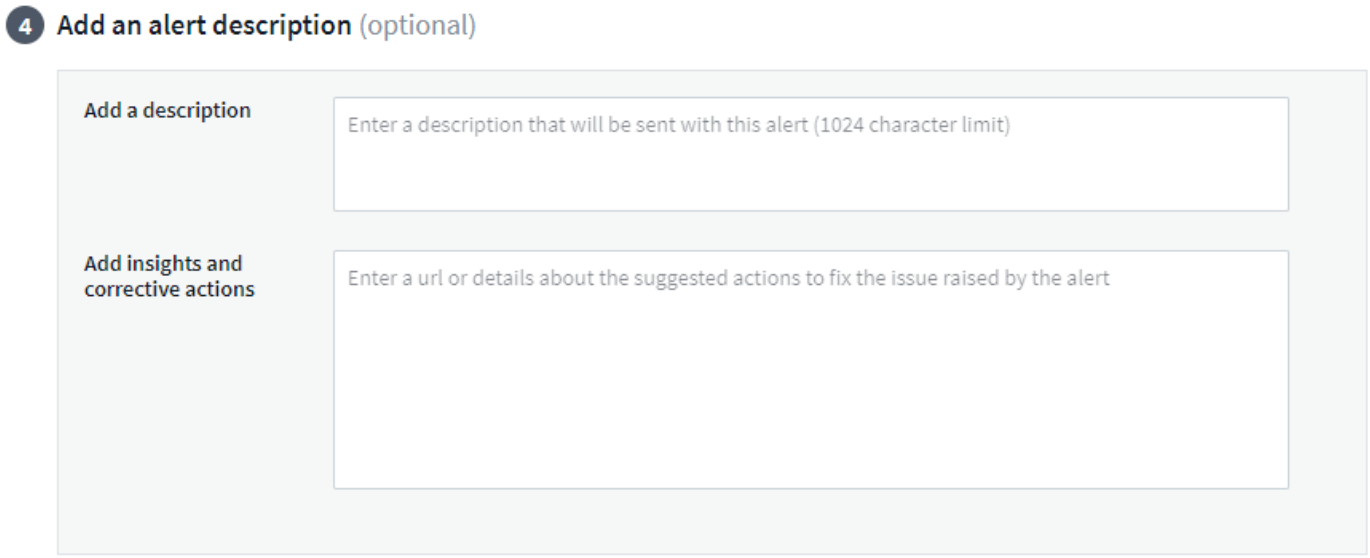
Agente Telegraf aggiornato

L'agente per l'inserimento dei dati di integrazione Telegraf è stato aggiornato alla versione 1.17.3, con miglioramenti delle prestazioni e della sicurezza. Gli utenti che desiderano effettuare l'aggiornamento possono fare riferimento alla sezione di aggiornamento appropriata del"Installazione dell'agente" documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza che sia richiesto alcun intervento da parte

dell'utente.

Aggiungere azioni correttive a un avviso

Ora puoi aggiungere una descrizione facoltativa, nonché ulteriori approfondimenti e/o azioni correttive durante la creazione o la modifica di un monitor compilando la sezione **Aggiungi una descrizione dell'avviso**. La descrizione verrà inviata con l'avviso. Il campo *insights and corrective actions* può fornire passaggi dettagliati e indicazioni per gestire gli avvisi e verrà visualizzato nella sezione di riepilogo della landing page dell'avviso.



API di Cloud Insights per tutte le edizioni

L'accesso API è ora disponibile in tutte le edizioni di Cloud Insights. Gli utenti dell'edizione Basic possono ora automatizzare le azioni per le unità di acquisizione e i collettori di dati, mentre gli utenti dell'edizione Standard possono interrogare le metriche e acquisire metriche personalizzate. L'edizione Premium continua a consentire l'utilizzo completo di tutte le categorie API.

Categoria API	Di base	Standard	Premio
Unità di acquisizione	✔	✔	✔
Raccolta dati	✔	✔	✔
Attività		✔	✔
Inserimento dati		✔	✔
Magazzino dati			✔

Per i dettagli sull'utilizzo dell'API, fare riferimento a"Documentazione API" .

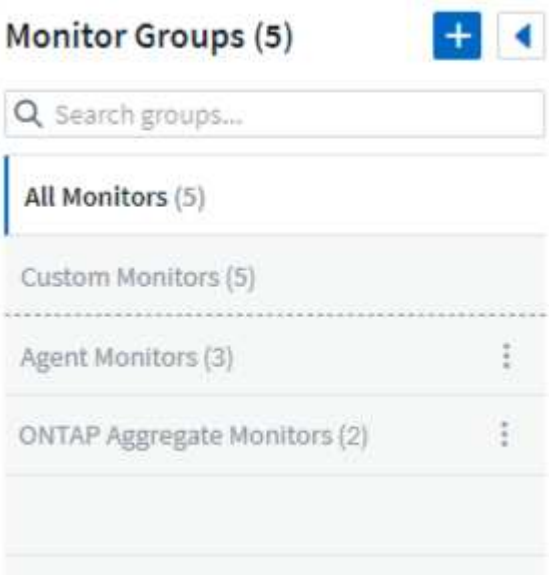
Aprile 2021

Gestione più semplice dei monitor

"Raggruppamento del monitor"semplifica la gestione dei monitor nel tuo ambiente. Ora è possibile raggruppare

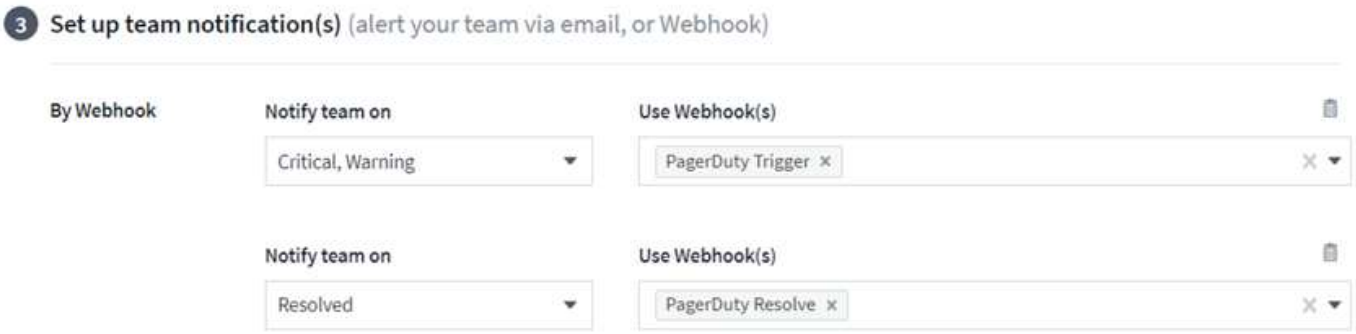
più monitor e metterli in pausa come se fossero uno solo. Ad esempio, se si verifica un aggiornamento su una serie di infrastrutture, è possibile sospendere gli avvisi da tutti quei dispositivi con un solo clic.

Monitora i gruppi è la prima parte di una nuova ed entusiasmante funzionalità che apporta una gestione migliorata dei dispositivi ONTAP a Cloud Insights.



Opzioni di avviso avanzate tramite webhook

Molte applicazioni commerciali supportano"Webhook" come interfaccia di input standard. Cloud Insights ora supporta molti di questi canali di distribuzione, fornendo modelli predefiniti per Slack, PagerDuty, Teams e Discord, oltre a fornire webhook generici personalizzabili per supportare molte altre applicazioni.



Identificazione del dispositivo migliorata

Per migliorare il monitoraggio e la risoluzione dei problemi, nonché per fornire report accurati, è utile comprendere i nomi dei dispositivi anziché i loro indirizzi IP o altri identificatori. Cloud Insights ora incorpora un modo automatico per identificare i nomi dei dispositivi host fisici e di archiviazione nell'ambiente, utilizzando un approccio basato su regole denominato**"Risoluzione del dispositivo"** , disponibile nel menu **Gestisci**.

Hai chiesto di più!

Una richiesta frequente da parte dei clienti è stata quella di avere più opzioni predefinite per visualizzare l'intervallo di dati, per questo abbiamo aggiunto le seguenti cinque nuove opzioni, ora disponibili in tutto il servizio tramite il selettore dell'intervallo di tempo:

- Ultimi 30 minuti
- Ultime 2 ore
- Ultime 6 ore
- Ultime 12 ore
- Ultimi 2 giorni

Più abbonamenti in un unico ambiente Cloud Insights

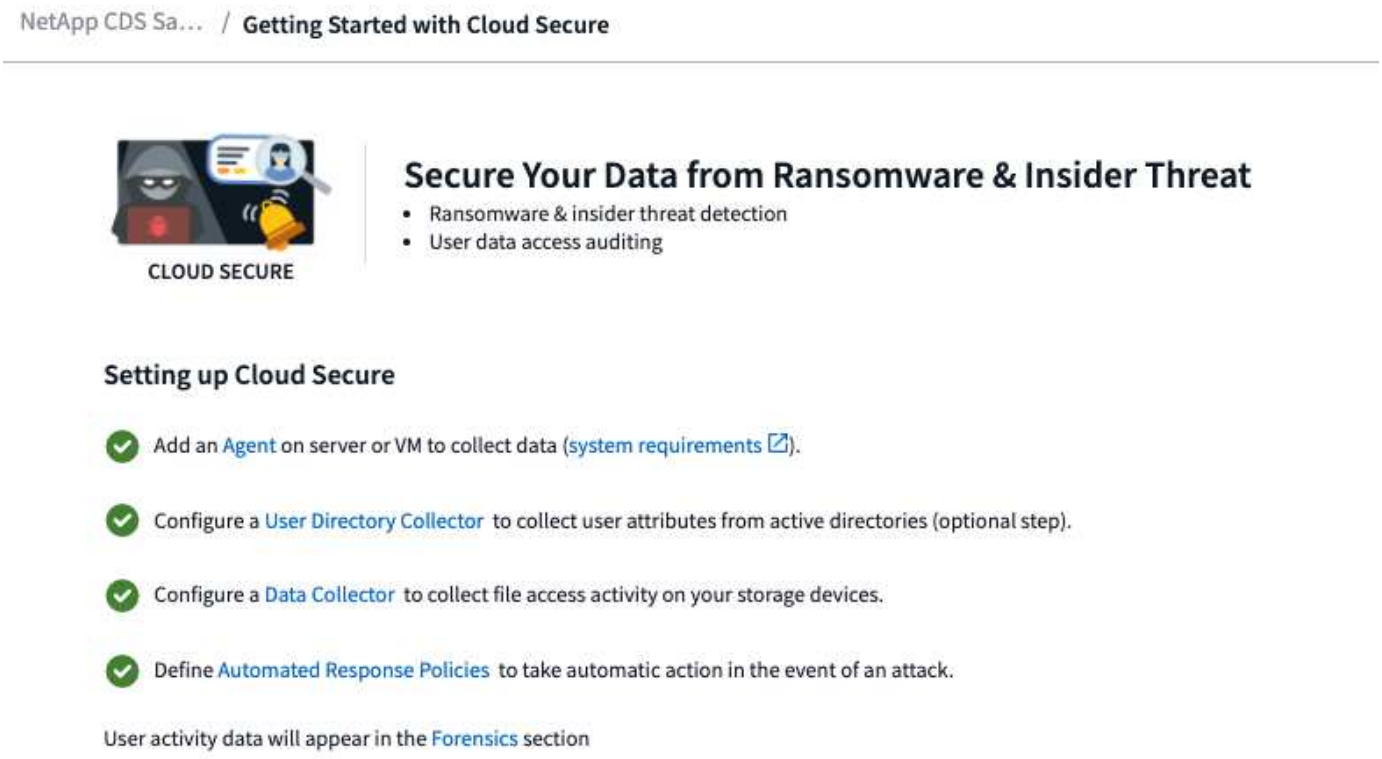
A partire dal 2 aprile, Cloud Insights supporta più abbonamenti dello stesso tipo di edizione per un cliente in una singola istanza Cloud Insights . Ciò consente ai clienti di contrarre parti del loro abbonamento a Cloud Insights con gli acquisti di infrastrutture. Per assistenza con più abbonamenti, contattare il reparto vendite NetApp .

Scegli il tuo percorso

Durante la configurazione di Cloud Insights, ora puoi scegliere se iniziare con Monitoraggio e avvisi oppure con Rilevamento ransomware e minacce interne. Cloud Insights configurerà l'ambiente iniziale in base al percorso scelto. È possibile configurare l'altro percorso in qualsiasi momento successivo.

Onboarding Cloud Secure più semplice

E iniziare a usare Cloud Secure è più facile che mai, grazie a una nuova checklist di configurazione dettagliata.



Come sempre, siamo lieti di ricevere i vostri suggerimenti! Inviateli a ng-cloudinsights-

customerfeedback@netapp.com.

Febbraio 2021

Agente Telegraf aggiornato

L'agente per l'inserimento dei dati di integrazione Telegraf è stato aggiornato alla versione 1.17.0, che include vulnerabilità e correzioni di bug.

Analizzatore dei costi del cloud

Scopri la potenza di Spot di NetApp con Cloud Cost, che fornisce un'analisi dettagliata dei costi passati, presenti e stimati, offrendo visibilità sull'utilizzo del cloud nel tuo ambiente. La dashboard dei costi del cloud offre una visione chiara delle spese del cloud e un'analisi dettagliata dei singoli carichi di lavoro, account e servizi.

Cloud Cost può aiutarti ad affrontare queste importanti sfide:

- Monitoraggio e monitoraggio delle spese cloud
- Identificazione degli sprechi e delle potenziali aree di ottimizzazione
- Consegna di elementi di azione eseguibili

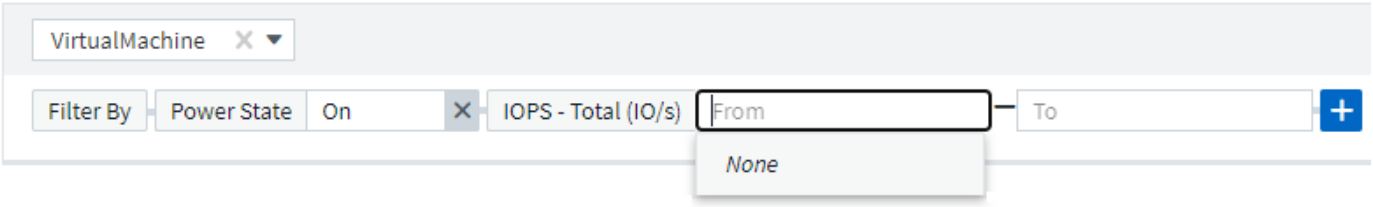
Cloud Cost è incentrato sul monitoraggio. Esegui l'upgrade all'account Spot by NetApp completo per abilitare il risparmio automatico sui costi e l'ottimizzazione dell'ambiente.

Ricerca di oggetti con valori nulli tramite filtri

Cloud Insights ora consente di cercare attributi e metriche con valori nulli/nessuno tramite l'uso di filtri. È possibile eseguire questo filtraggio su qualsiasi attributo/metrica nei seguenti punti:

- Nella pagina Query
- Nei widget della dashboard e nelle variabili di pagina
- Nella pagina dell'elenco degli avvisi
- Durante la creazione dei monitor

Per filtrare i valori nulli/nessuno, è sufficiente selezionare l'opzione *Nessuno* quando appare nel menu a discesa del filtro appropriato.



Supporto multi-regione

A partire da oggi offriamo il servizio Cloud Insights in diverse regioni del mondo, il che semplifica le prestazioni e aumenta la sicurezza per i clienti con sede al di fuori degli Stati Uniti. Cloud Insights/ Cloud Secure archivia

le informazioni in base alla regione in cui è stato creato l'ambiente.

Clic"Qui" per maggiori informazioni.

Gennaio 2021

Ulteriori metriche ONTAP rinominate

Nell'ambito del nostro continuo impegno per migliorare l'efficienza della raccolta dati dai sistemi ONTAP , le seguenti metriche ONTAP sono state rinominate.

Se hai già dei widget o delle query della dashboard che utilizzano una di queste metriche, dovrai modificarli o ricrearli per utilizzare i nuovi nomi delle metriche.

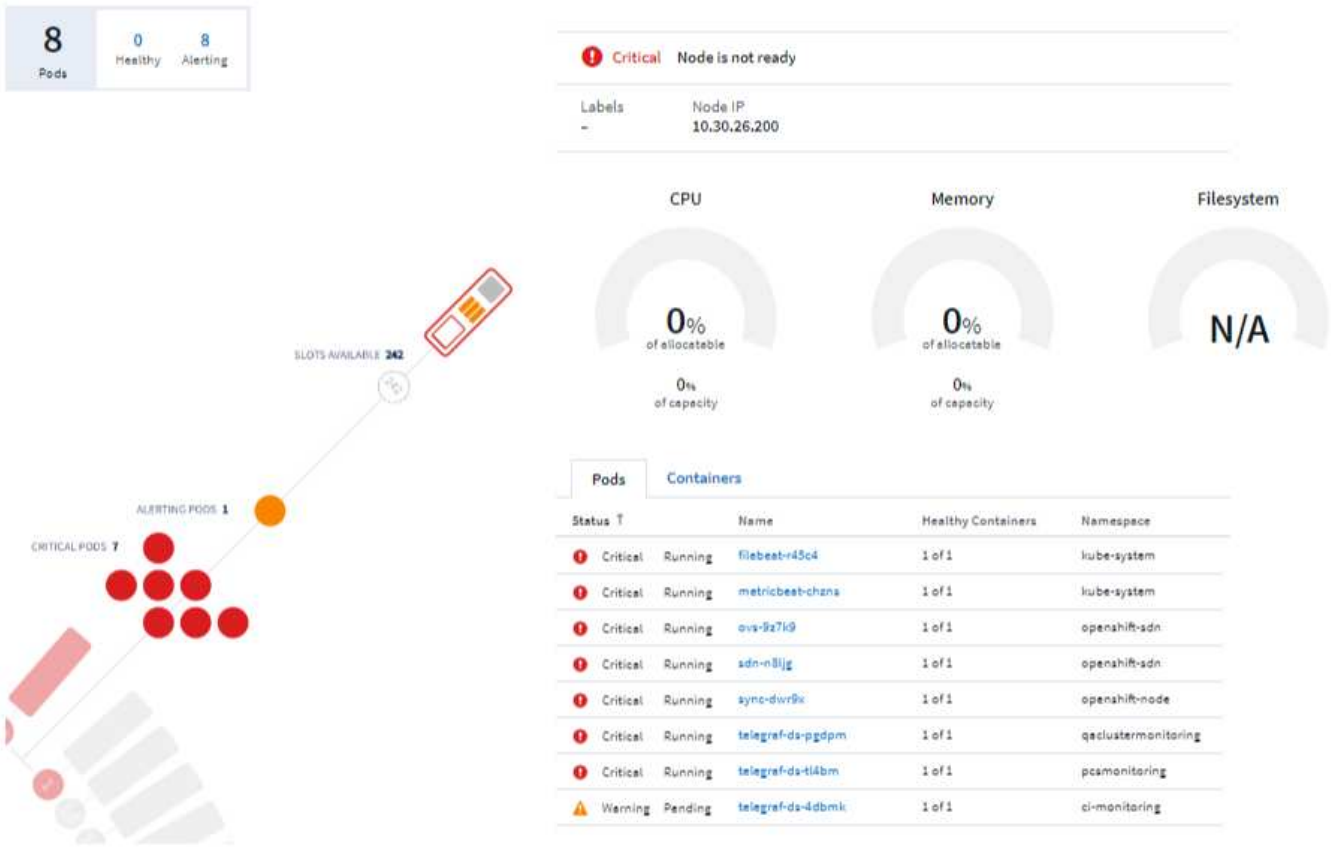
Nome metrica precedente	Nuovo nome metrica
netapp_ontap.disk_constituent.total_transfers	netapp_ontap.disk_constituent.total_iops
netapp_ontap.disk.total_transfers	netapp_ontap.disk.total_iops
netapp_ontap.fcp_lif.read_data	netapp_ontap.fcp_lif.read_throughput
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.write_throughput
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.read_throughput
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.write_throughput
netapp_ontap.lif.recv_data	netapp_ontap.lif.recv_throughput
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
netapp_ontap.lun.read_data	netapp_ontap.lun.read_throughput
netapp_ontap.lun.write_data	netapp_ontap.lun.write_throughput
netapp_ontap.nic_common.rx_bytes	netapp_ontap.nic_common.rx_throughput
netapp_ontap.nic_common.tx_bytes	netapp_ontap.nic_common.tx_throughput
netapp_ontap.path.read_data	netapp_ontap.path.read_throughput
netapp_ontap.path.write_data	netapp_ontap.path.write_throughput
netapp_ontap.path.total_data	netapp_ontap.path.total_throughput
netapp_ontap.policy_group.read_data	netapp_ontap.policy_group.read_throughput
netapp_ontap.policy_group.write_data	netapp_ontap.policy_group.write_throughput
netapp_ontap.policy_group.other_data	netapp_ontap.policy_group.other_throughput
netapp_ontap.policy_group.total_data	netapp_ontap.policy_group.total_throughput
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.disk_throughput_read
netapp_ontap.system_node.disk_data_written	netapp_ontap.system_node.disk_throughput_written
lettura_dati_hdd_netapp_ontap.system_node	netapp_ontap.system_node.hdd_throughput_read
netapp_ontap.system_node.hdd_data_written	netapp_ontap.system_node.hdd_throughput_scritto

Nome metrica precedente	Nuovo nome metrica
lettura_dati_ssd_netapp_ontap.system_node	lettura_throughput_ssd_netapp_ontap.system_node
netapp_ontap.system_node.ssd_data_written	netapp_ontap.system_node.ssd_throughput_written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
netapp_ontap.system_node.fcp_data_recv	netapp_ontap.system_node.fcp_throughput_recv
netapp_ontap.system_node.fcp_data_sent	netapp_ontap.system_node.fcp_throughput_sent
netapp_ontap.volume_node.cifs_read_data	netapp_ontap.volume_node.cifs_read_throughput
netapp_ontap.volume_node.cifs_write_data	netapp_ontap.volume_node.cifs_write_throughput
netapp_ontap.volume_node.nfs_read_data	netapp_ontap.volume_node.nfs_read_throughput
netapp_ontap.volume_node.nfs_write_data	netapp_ontap.volume_node.nfs_write_throughput
netapp_ontap.volume_node.iscsi_read_data	netapp_ontap.volume_node.iscsi_read_throughput
netapp_ontap.volume_node.iscsi_write_data	netapp_ontap.volume_node.iscsi_write_throughput
netapp_ontap.volume_node.fcp_read_data	netapp_ontap.volume_node.fcp_read_throughput
netapp_ontap.volume_node.fcp_write_data	netapp_ontap.volume_node.fcp_write_throughput
netapp_ontap.volume.read_data	netapp_ontap.volume.lettura_throughput
netapp_ontap.volume.write_data	netapp_ontap.volume.write_throughput
netapp_ontap.workload.read_data	netapp_ontap.workload.read_throughput
netapp_ontap.workload.write_data	netapp_ontap.workload.write_throughput
netapp_ontap.workload_volume.read_data	netapp_ontap.workload_volume.read_throughput
netapp_ontap.workload_volume.write_data	netapp_ontap.volume_carico_di_lavoro.write_throughput

Nuovo Kubernetes Explorer

IL"Esploratore Kubernetes" fornisce una semplice visualizzazione della topologia dei cluster Kubernetes, consentendo anche ai non esperti di identificare rapidamente problemi e dipendenze, dal livello del cluster fino al contenitore e all'archiviazione.

È possibile esplorare un'ampia gamma di informazioni utilizzando i dettagli dettagliati di Kubernetes Explorer per lo stato, l'utilizzo e l'integrità di cluster, nodi, pod, container e storage nel tuo ambiente Kubernetes.



Dicembre 2020

Installazione di Kubernetes più semplice

L'installazione di Kubernetes Agent è stata semplificata per richiedere meno interazioni da parte dell'utente. "Installazione dell'agente Kubernetes" ora include la raccolta dati Kubernetes.

Novembre 2020

Dashboard aggiuntive

Le seguenti nuove dashboard incentrate su ONTAP sono state aggiunte alla galleria e sono disponibili per l'importazione:

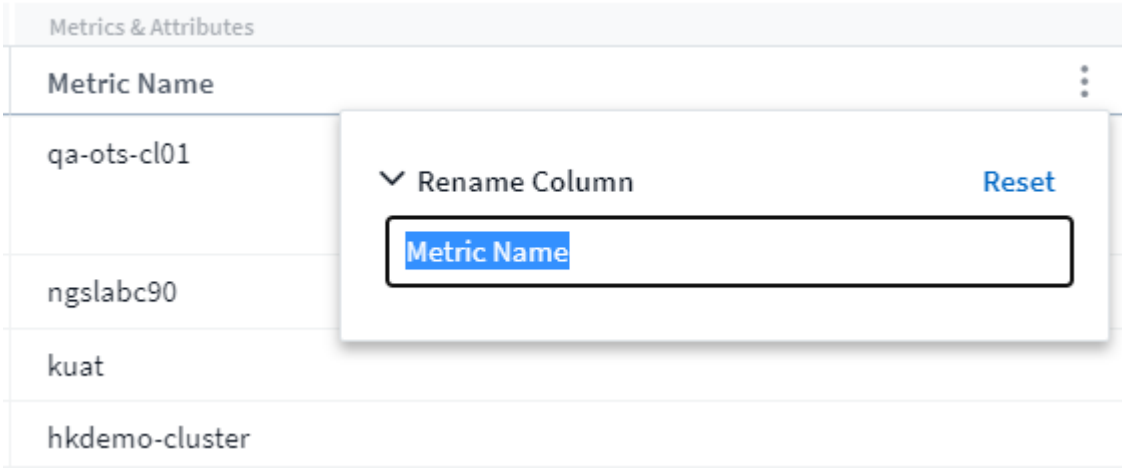
- ONTAP: Prestazioni e capacità aggregate
- ONTAP FAS/ AFF - Utilizzo della capacità
- ONTAP FAS/ AFF - Capacità del cluster
- ONTAP FAS/ AFF - Efficienza
- ONTAP FAS/ AFF - Prestazioni FlexVol

- ONTAP FAS/ AFF - Punti operativi/ottimali del nodo
- ONTAP FAS/ AFF - Efficienze di capacità pre-post
- ONTAP: attività della porta di rete
- ONTAP: Prestazioni dei protocolli dei nodi
- ONTAP: Prestazioni del carico di lavoro del nodo (frontend)
- ONTAP: Processore
- ONTAP: prestazioni del carico di lavoro SVM (frontend)
- ONTAP: Prestazioni del carico di lavoro del volume (frontend)

Rinomina colonna nei widget tabella

È possibile rinominare le colonne nella sezione *Metriche e attributi* di un widget tabella aprendo il widget in modalità di modifica e facendo clic sul menu nella parte superiore della colonna. Inserisci il nuovo nome e fai clic su *Salva* oppure fai clic su *Reimposta* per ripristinare il nome originale della colonna.

Si noti che questo influisce solo sul nome visualizzato della colonna nel widget della tabella; il nome della metrica/attributo non cambia nei dati sottostanti.



Ottobre 2020

Espansione predefinita dei dati di integrazione

Il raggruppamento dei widget della tabella ora consente espansioni predefinite delle metriche Kubernetes, ONTAP Advanced Data e Agent Node. Ad esempio, se raggruppi i *Nodi* Kubernetes per *Cluster*, vedrai una riga nella tabella per ogni cluster. È quindi possibile espandere ogni riga del cluster per visualizzare un elenco degli oggetti Node.

Supporto tecnico dell'edizione base

Il supporto tecnico è ora disponibile per gli abbonati a Cloud Insights Basic Edition, oltre che alle edizioni Standard e Premium. Inoltre, Cloud Insights ha semplificato il flusso di lavoro per la creazione di un ticket di supporto NetApp .

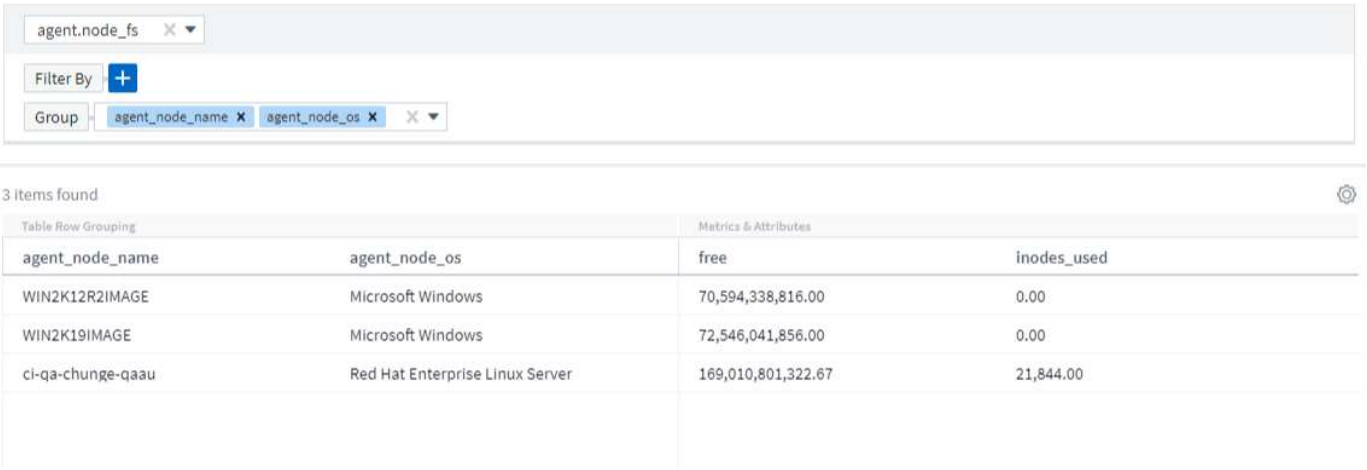
API pubblica Cloud Secure

Cloud Secure supporta"API REST" per accedere alle informazioni su attività e avvisi. Ciò viene realizzato tramite l'uso di token di accesso API, creati tramite l'interfaccia utente di amministrazione Cloud Secure , che vengono poi utilizzati per accedere alle API REST. La documentazione Swagger per queste API REST è integrata con Cloud Secure.

Settembre 2020

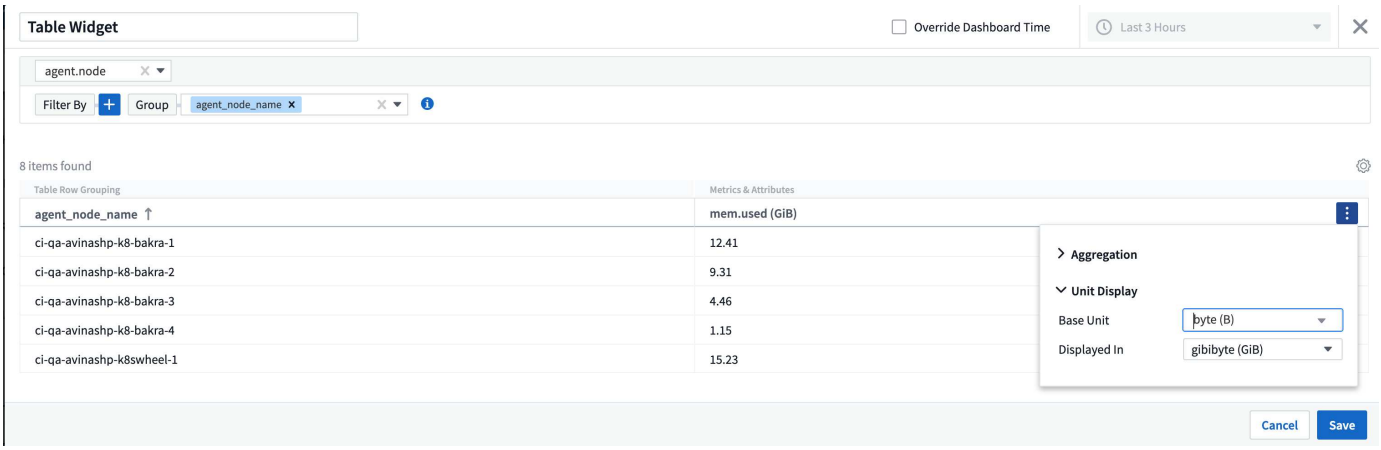
Pagina di query con dati di integrazione

La pagina Query di Cloud Insights supporta i dati di integrazione (ad esempio da Kubernetes, ONTAP Advanced Metrics, ecc.). Quando si lavora con i dati di integrazione, la tabella dei risultati della query mostra una vista "a schermo diviso", con l'oggetto/raggruppamento sul lato sinistro e i dati dell'oggetto (attributi/metriche) sul lato destro. È anche possibile scegliere più attributi per raggruppare i dati di integrazione.



Formattazione della visualizzazione dell'unità nel widget Tabella

La formattazione della visualizzazione delle unità è ora disponibile nei widget Tabella per le colonne che visualizzano dati metrici/contatori (ad esempio, gigabyte, MB/secondo, ecc.). Per modificare l'unità di visualizzazione di una metrica, fare clic sul menu "tre puntini" nell'intestazione della colonna e selezionare "Visualizzazione unità". Puoi scegliere tra tutte le unità disponibili. Le unità disponibili variano a seconda del tipo di dati metrici nella colonna visualizzata.



Pagina dei dettagli dell'unità di acquisizione

Le unità di acquisizione ora hanno una propria landing page, che fornisce dettagli utili per ciascuna AU e informazioni utili per la risoluzione dei problemi. IL"Pagina dei dettagli AU" fornisce link ai raccoglitori di dati dell'UA nonché utili informazioni sullo stato.

Dipendenza Docker Cloud Secure rimossa

La dipendenza di Cloud Secure da Docker è stata rimossa. Docker non è più necessario per l'installazione dell'agente Cloud Secure .

Segnalazione dei ruoli utente

Se disponi di Cloud Insights Premium Edition con Reporting, ogni utente Cloud Insights nel tuo ambiente avrà anche un accesso Single Sign-On (SSO) all'applicazione Reporting (ad esempio Cognos); cliccando sul collegamento **Report** nel menu, accederanno automaticamente a Reporting.

Il loro ruolo utente in Cloud Insights determina il loro"Ruolo utente di segnalazione" :

Ruolo Cloud Insights	Ruolo di segnalazione	Autorizzazioni di segnalazione
Ospite	Consumatore	È possibile visualizzare, pianificare ed eseguire report e impostare preferenze personali, come quelle relative a lingue e fusi orari. I consumatori non possono creare report o svolgere attività amministrative.
Utente	Autore	Può eseguire tutte le funzioni del consumatore, nonché creare e gestire report e dashboard.
Amministratore	Amministratore	Può eseguire tutte le funzioni dell'autore nonché tutte le attività amministrative, come la configurazione dei report e l'arresto e il riavvio delle attività di reporting.

Cloud Insights Reporting è disponibile per ambienti da 500 MU o più.

Se sei un attuale cliente Premium Edition e desideri conservare i tuoi report, leggi questo"nota importante per i clienti esistenti" .

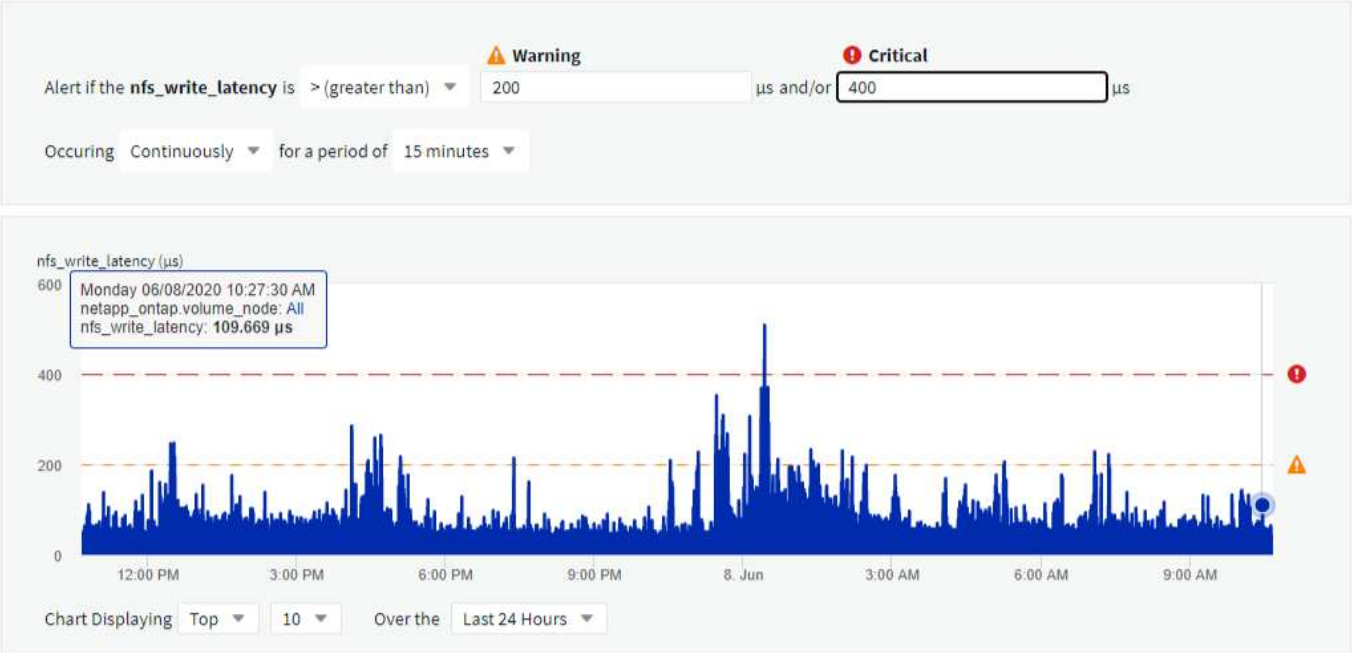
Nuova categoria API per l'inserimento dei dati

Cloud Insights ha aggiunto una categoria API **Data Ingestion**, offrendoti un maggiore controllo sui dati e sugli agenti personalizzati. La documentazione dettagliata per questa e altre categorie API è disponibile in Cloud Insights andando su **Amministrazione > Accesso API** e cliccando sul link *Documentazione API*. È anche possibile allegare un commento all'AU nel campo Nota, visualizzato sia nella pagina dei dettagli dell'AU che nella pagina dell'elenco delle AU.

Agosto 2020

Monitoraggio e allerta

Oltre all'attuale possibilità di impostare criteri di prestazioni per oggetti di archiviazione, VM, EC2 e porte, Cloud Insights Standard Edition ora include la possibilità di"configurare i monitor" per soglie sui dati di integrazione per Kubernetes, metriche avanzate ONTAP e plugin Telegraf. È sufficiente creare un monitor per ogni metrica di oggetto per cui si desidera attivare gli avvisi, impostare le condizioni per le soglie di livello di avviso o di livello critico e specificare i destinatari e-mail desiderati per ciascun livello. Puoi quindi"visualizzare e gestire gli avvisi" per monitorare le tendenze o risolvere i problemi.



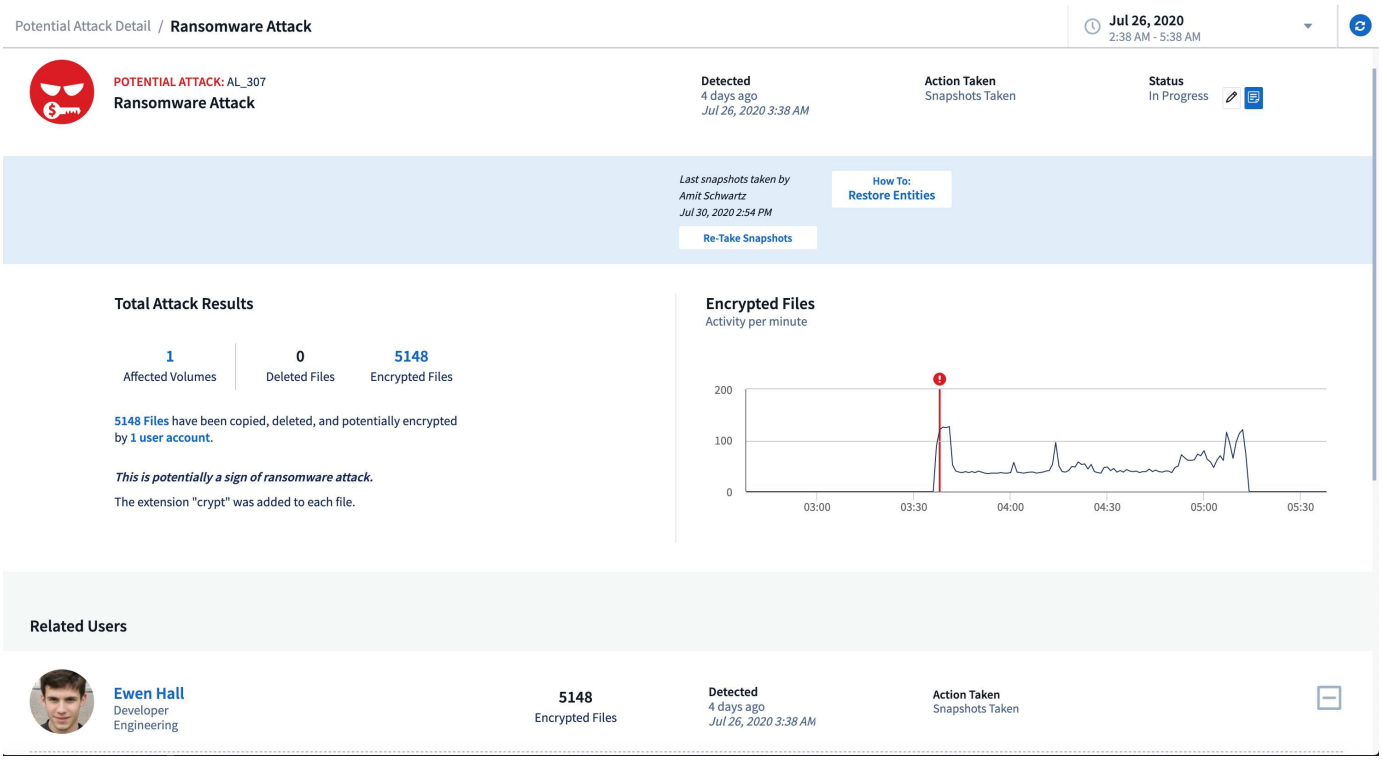
Luglio 2020

Cloud Secure *Esegui un'istantanea* **Azione**

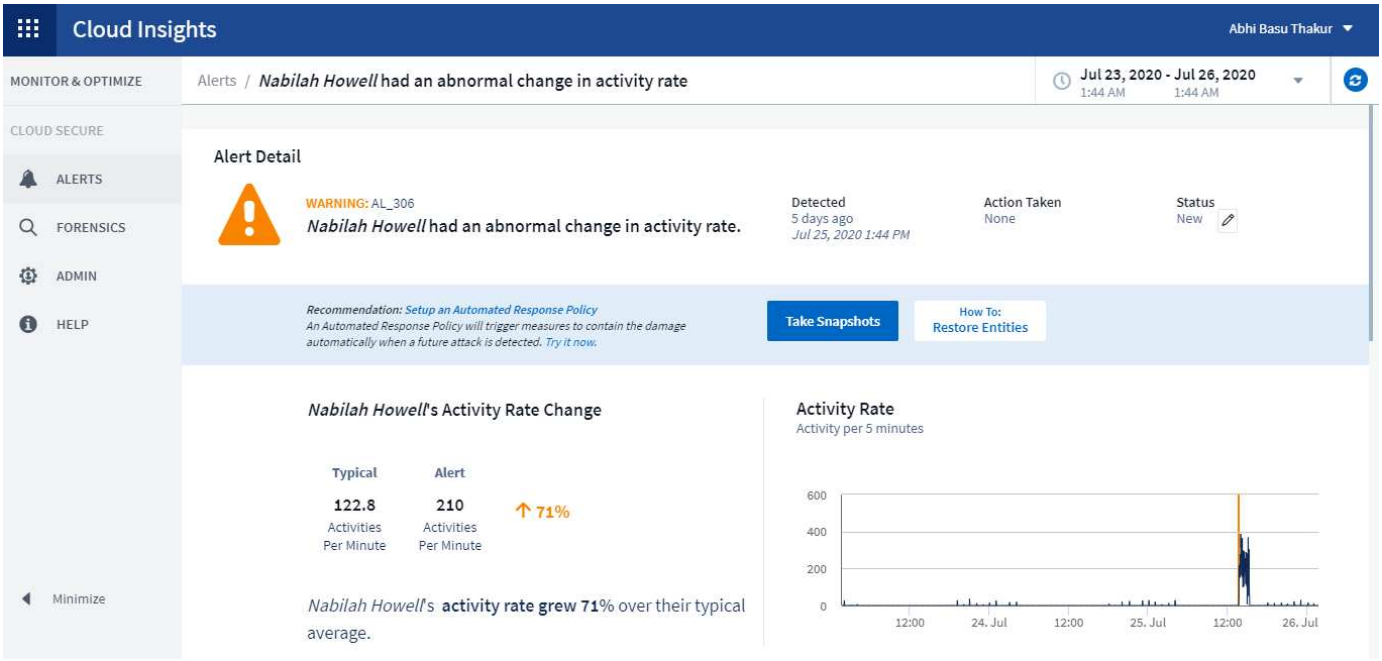
Cloud Secure protegge i tuoi dati eseguendo automaticamente uno snapshot quando viene rilevata un'attività dannosa, garantendo così un backup sicuro dei tuoi dati.

È possibile definire policy di risposta automatizzate che creano uno snapshot quando viene rilevato un attacco ransomware o altre attività anomale dell'utente. È anche possibile acquisire manualmente uno snapshot dalla pagina di avviso.

Istantanea automatica scattata:



Istantanea manuale:



Aggiornamenti metrici/contatori

I seguenti contatori di capacità sono disponibili per l'uso nell'interfaccia utente Cloud Insights e nell'API REST. In precedenza questi contatori erano disponibili solo per Data Warehouse/Reporting.

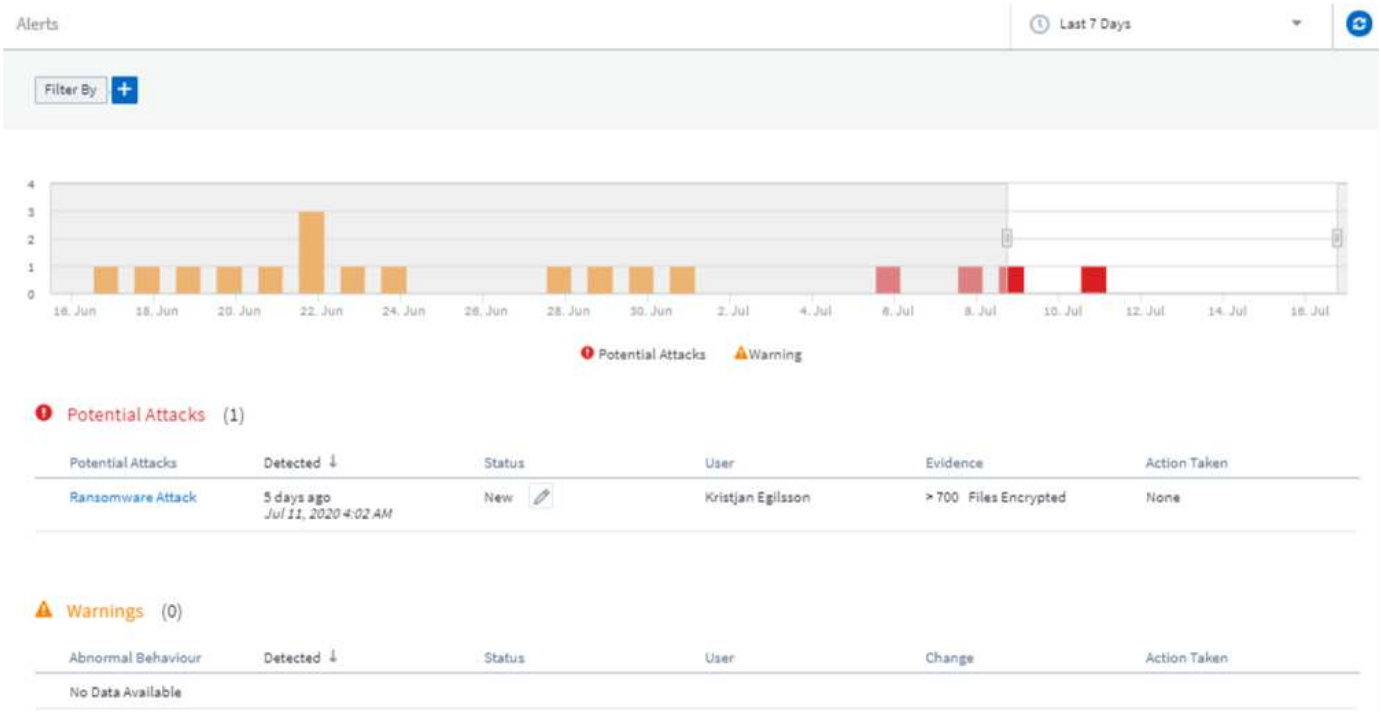
Tipo di oggetto	Contatore
Magazzinaggio	Capacità - Capacità grezza di riserva - Capacità grezza non riuscita
Pool di archiviazione	Capacità dati - Capacità dati utilizzata - Altra capacità totale - Altra capacità utilizzata - Capacità totale - Capacità grezza - Limite flessibile
Volume interno	Capacità dati - Capacità dati utilizzata - Totale Altra capacità - Utilizzata Altra capacità - Totale Capacità di clonazione salvata - Totale

Rilevamento di potenziali attacchi Cloud Secure

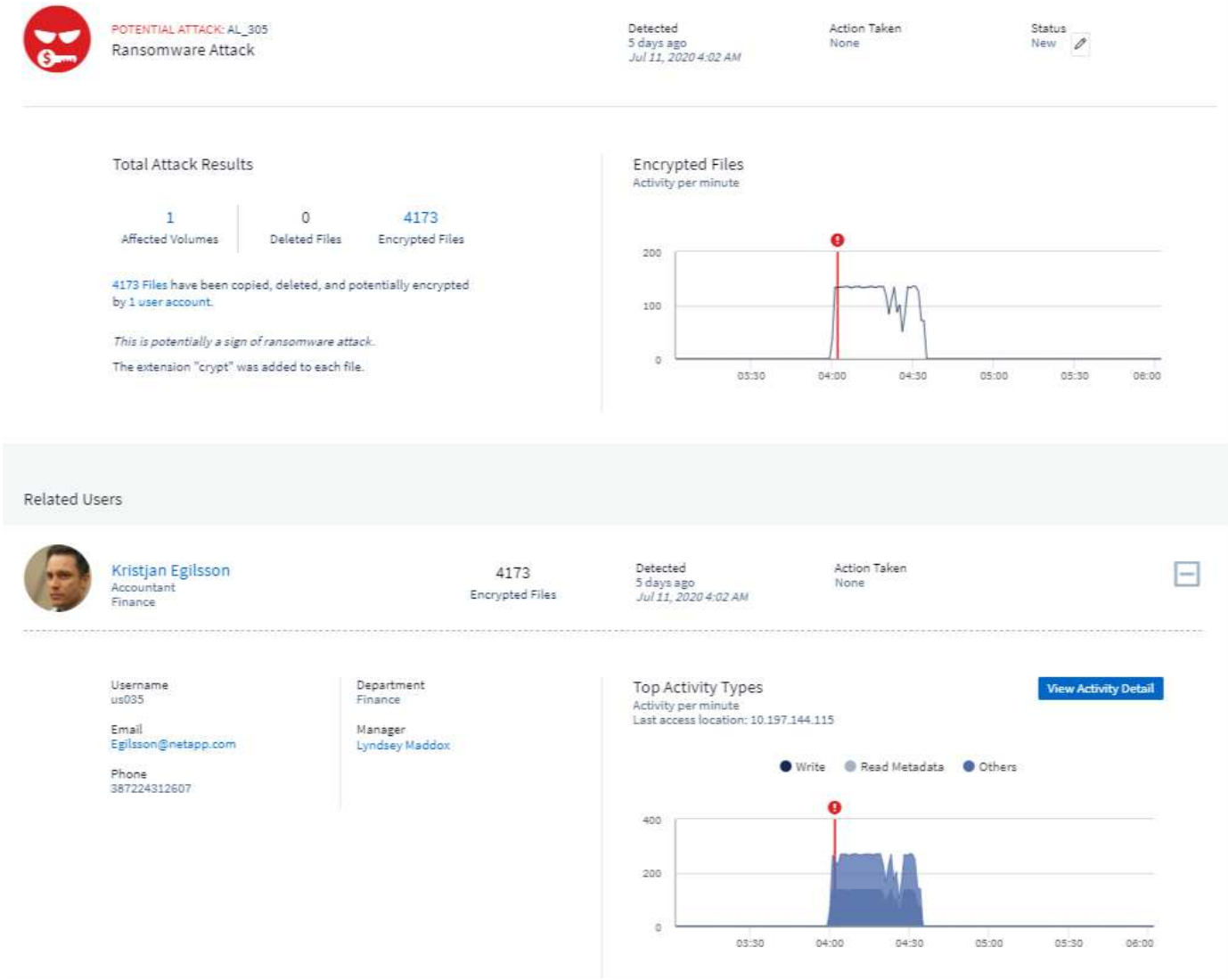
Cloud Secure ora rileva potenziali attacchi come il ransomware. Fare clic su un avviso nella pagina Elenco avvisi per aprire una pagina di dettagli che mostra quanto segue:

- Ora dell'attacco
- Attività associata dell'utente e del file
- Azione intrapresa
- Informazioni aggiuntive per aiutare a individuare possibili violazioni della sicurezza

Pagina di avvisi che mostra un potenziale attacco ransomware:



Pagina dettagliata per un potenziale attacco ransomware:



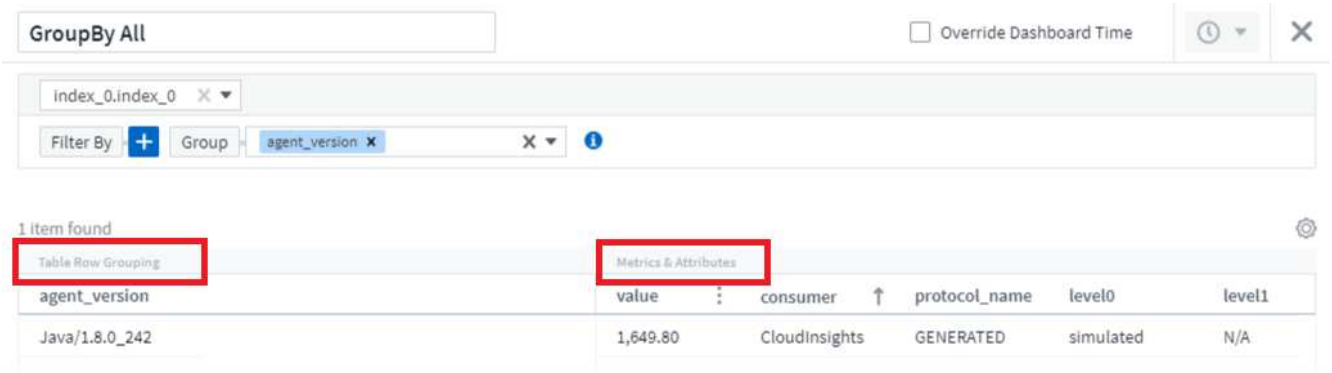
Iscriviti alla Premium Edition tramite AWS

Durante la prova di Cloud Insights, puoi"auto-iscrizione" tramite AWS Marketplace a Cloud Insights Standard Edition o Premium Edition. In precedenza, era possibile auto-iscriversi solo tramite AWS Marketplace alla Standard Edition.

Widget tabella migliorato

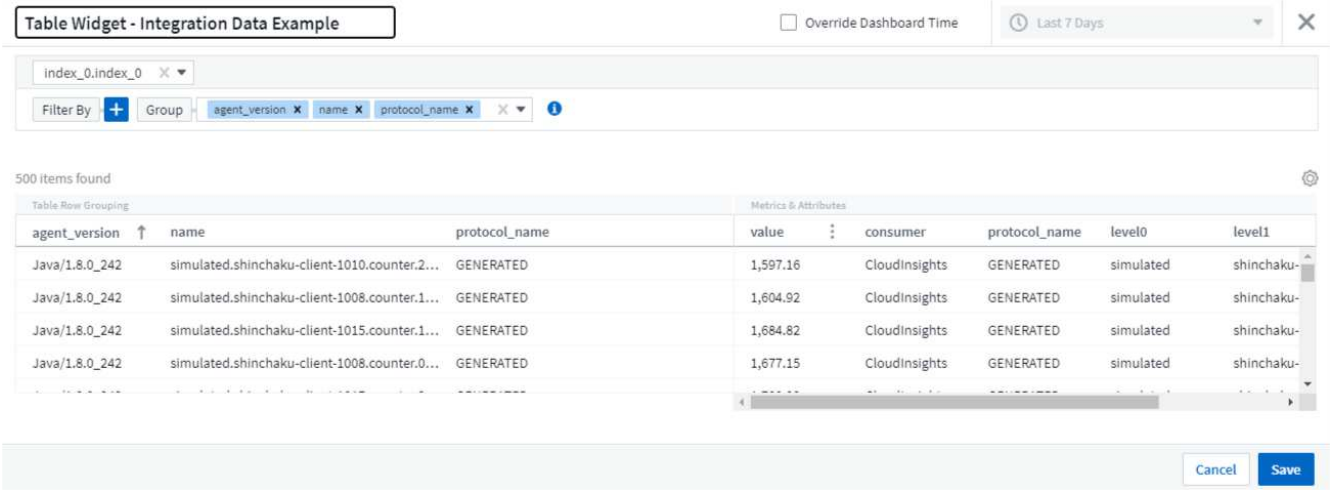
Il widget Tabella della pagina dashboard/risorse include i seguenti miglioramenti:

- Visualizzazione "schermo diviso": i widget tabella visualizzano l'oggetto/raggruppamento sul lato sinistro e i dati dell'oggetto (attributi/metriche) sul lato destro.



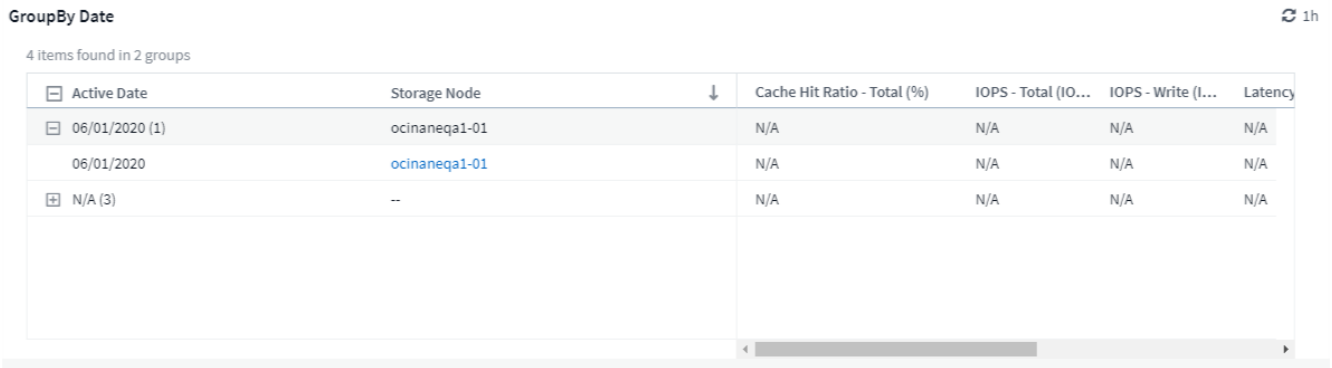
- Raggruppamento di più attributi: per i dati di integrazione (Kubernetes, ONTAP Advanced Metrics, Docker, ecc.), è possibile scegliere più attributi per il raggruppamento. I dati vengono visualizzati in base agli attributi di raggruppamento scelti.

  Raggruppamento con dati di integrazione (mostrato in modalità di modifica):



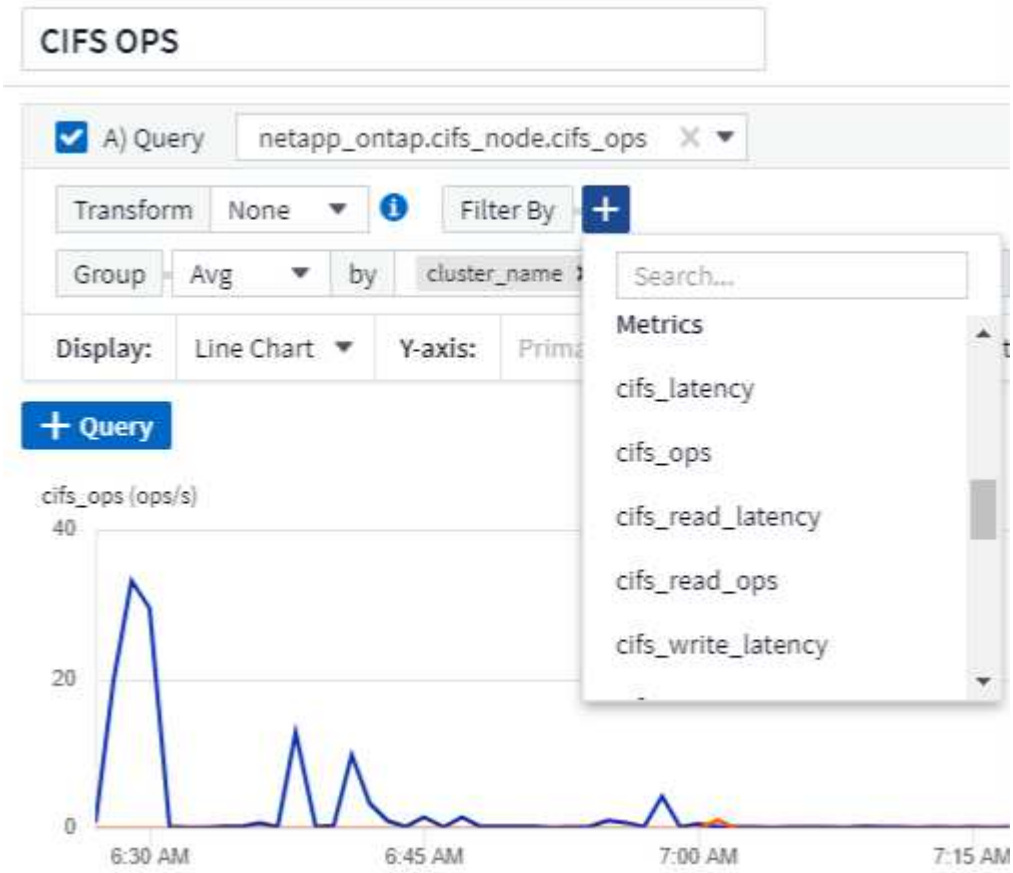
- Il raggruppamento dei dati dell'infrastruttura (archiviazione, EC2, VM, porte, ecc.) avviene tramite un singolo attributo, come in precedenza. Quando si raggruppa in base a un attributo che non è l'oggetto, la tabella consente di espandere la riga del gruppo per visualizzare tutti gli oggetti al suo interno.

  Raggruppamento con dati infrastrutturali (mostrati in modalità di visualizzazione):

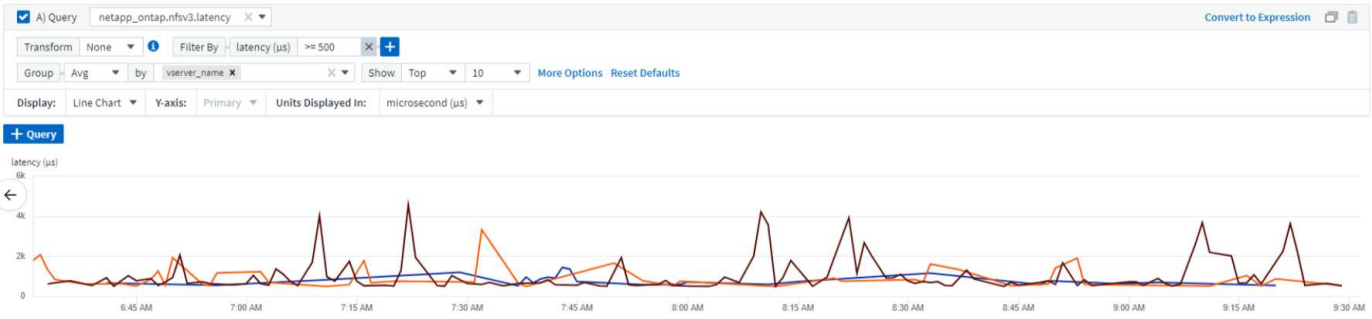


Filtraggio delle metriche

Oltre a filtrare in base agli attributi di un oggetto in un widget, ora puoi filtrare anche in base alle metriche.



Quando si lavora con dati di integrazione (Kubernetes, ONTAP Advanced Data, ecc.), il filtraggio delle metriche rimuove i punti dati individuali/non corrispondenti dalla serie di dati tracciati, a differenza dei dati dell'infrastruttura (archiviazione, VM, porte, ecc.) in cui i filtri agiscono sul valore aggregato della serie di dati e potenzialmente rimuovono l'intero oggetto dal grafico.

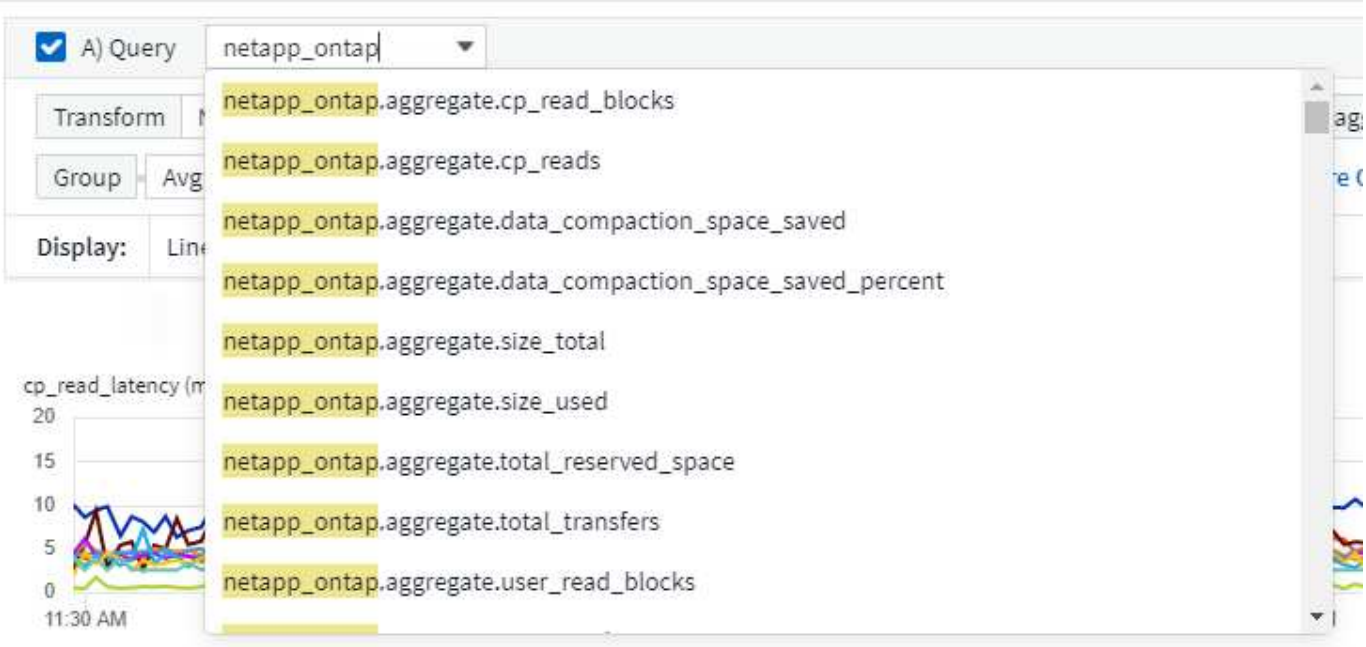


Dati contatore avanzati ONTAP

Cloud Insights sfrutta i dati avanzati dei contatori specifici di ONTAP di NetApp, che forniscono una serie di contatori e metriche raccolti dai dispositivi ONTAP . I dati dei contatori avanzati ONTAP sono disponibili per tutti i clienti NetApp ONTAP . Queste metriche consentono una visualizzazione personalizzata e ampia nei widget e nelle dashboard Cloud Insights .

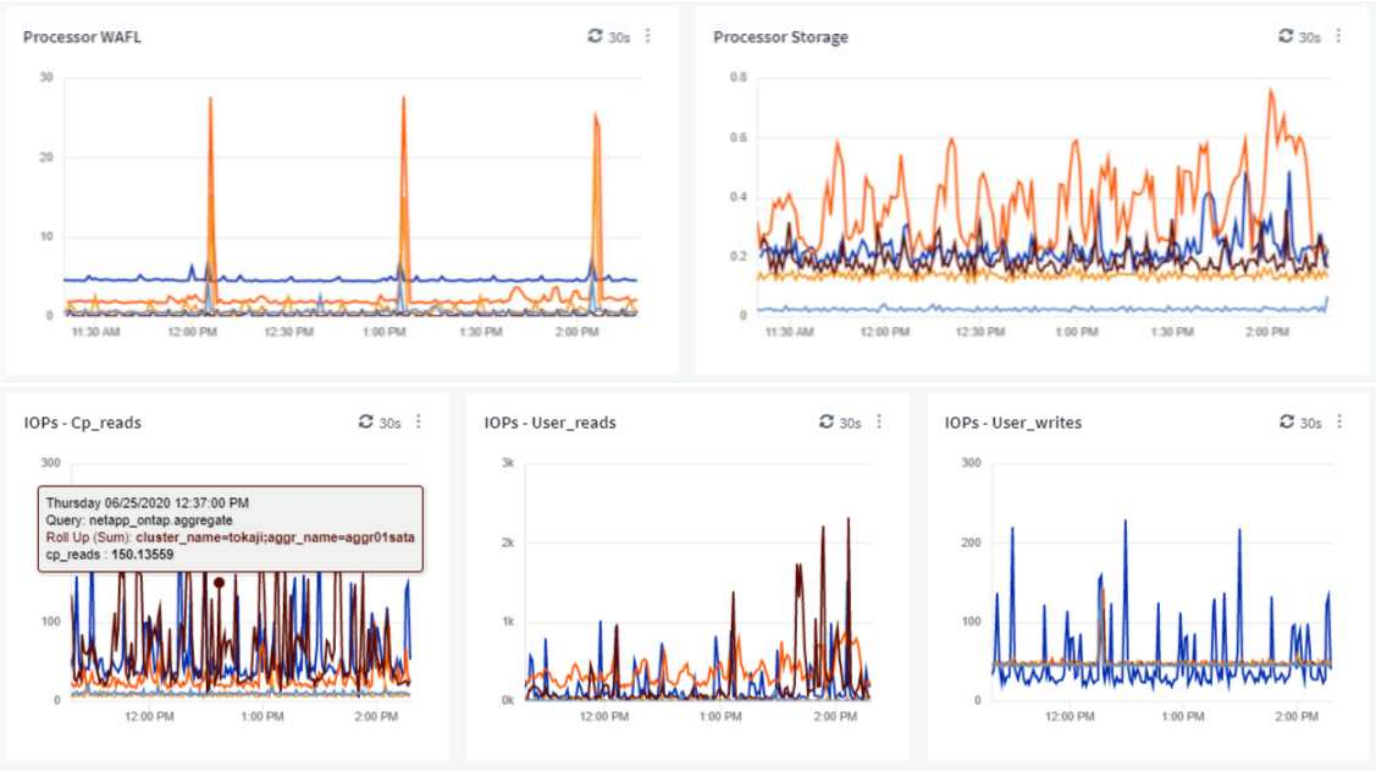
È possibile trovare i contatori avanzati ONTAP cercando "netapp_ontap" nella query del widget e selezionando

uno dei contatori.



Puoi perfezionare la ricerca digitando parti aggiuntive del nome del contatore. Per esempio:

- *vita*
- *aggregato*
- *offbox_vscan_server*
- e altro ancora



Si prega di notare quanto segue:

- La raccolta dati avanzata sarà abilitata per impostazione predefinita per i nuovi collettori dati ONTAP . Per abilitare la raccolta dati avanzata per i tuoi raccoglitori dati ONTAP esistenti, modifica il raccoglitore dati ed espandi la sezione *Configurazione avanzata*.
- La raccolta dati avanzata non è disponibile per ONTAP a 7 modalità.

Dashboard dei contatori avanzati

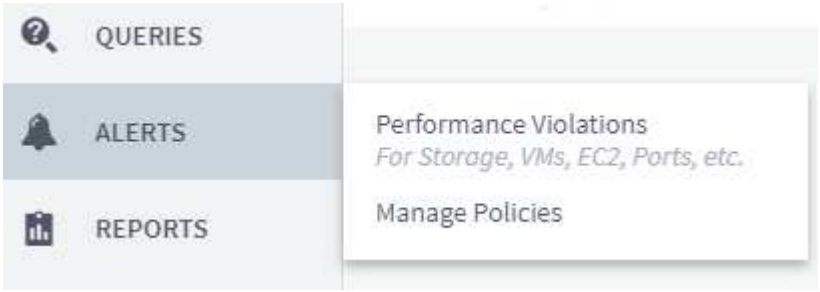
Cloud Insights è dotato di una serie di dashboard predefinite per aiutarti a iniziare a visualizzare i contatori avanzati ONTAP per argomenti quali *Prestazioni aggregate*, *Carico di lavoro del volume*, *Attività del processore* e altro ancora. Se è configurato almeno un raccoglitore dati ONTAP , è possibile importarlo dalla Galleria dashboard in qualsiasi pagina dell'elenco dashboard.

Saperne di più

Ulteriori informazioni su ONTAP Advanced Data sono disponibili ai seguenti xref:./*
https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest(Nota: sarà necessario accedere al supporto NetApp)
* https://nabox.org/faq/

Menu Norme e violazioni

Le policy e le violazioni delle prestazioni ora si trovano nel menu **Avvisi**. Le funzionalità relative alle norme e alle violazioni rimangono invariate.



Agente Telegraf aggiornato

L'agente per l'inserimento dei dati di integrazione Telegraf è stato aggiornato a"versione 1.14" , che include correzioni di bug, correzioni di sicurezza e nuovi plugin.

Nota: quando si configura un raccoglitore dati Kubernetes sulla piattaforma Kubernetes, potrebbe essere visualizzato un errore "HTTP status 403 Forbidden" nel registro, a causa di autorizzazioni insufficienti nell'attributo "clusterrole".

Per risolvere questo problema, aggiungere le seguenti righe evidenziate alla sezione *rules:* del clusterrole endpoint-access, quindi riavviare i pod Telegraf.

```
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  attributeRestrictions: null
  resources:
  - nodes/metrics
  - nodes/proxy     <== Add this line
  - nodes/stats
  - pods            <== Add this line
  verbs:
  - get
  - list            <== Add this line
```

Giugno 2020

Segnalazione errori semplificata del Data Collector

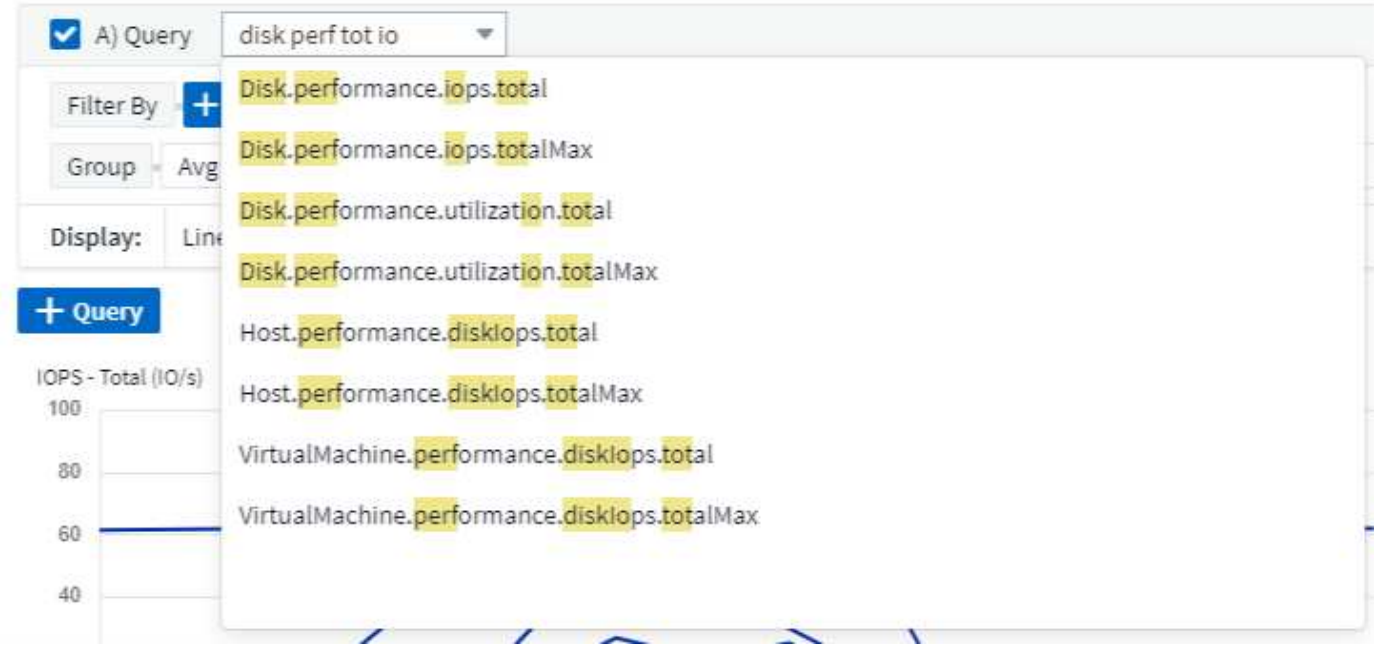
Segnalare un errore del raccoglitore dati è più semplice con il pulsante *Invia segnalazione errore* nella pagina del raccoglitore dati. Facendo clic sul pulsante, vengono inviate a NetApp informazioni di base sull'errore e viene avviata un'indagine sul problema. Una volta premuto, Cloud Insights riconosce che NetApp è stata avvisata e il pulsante Segnalazione errori viene disabilitato per indicare che è stato inviato un rapporto di errore per quel raccoglitore di dati. Il pulsante rimane disattivato finché la pagina del browser non viene aggiornata.

Miglioramenti dei widget

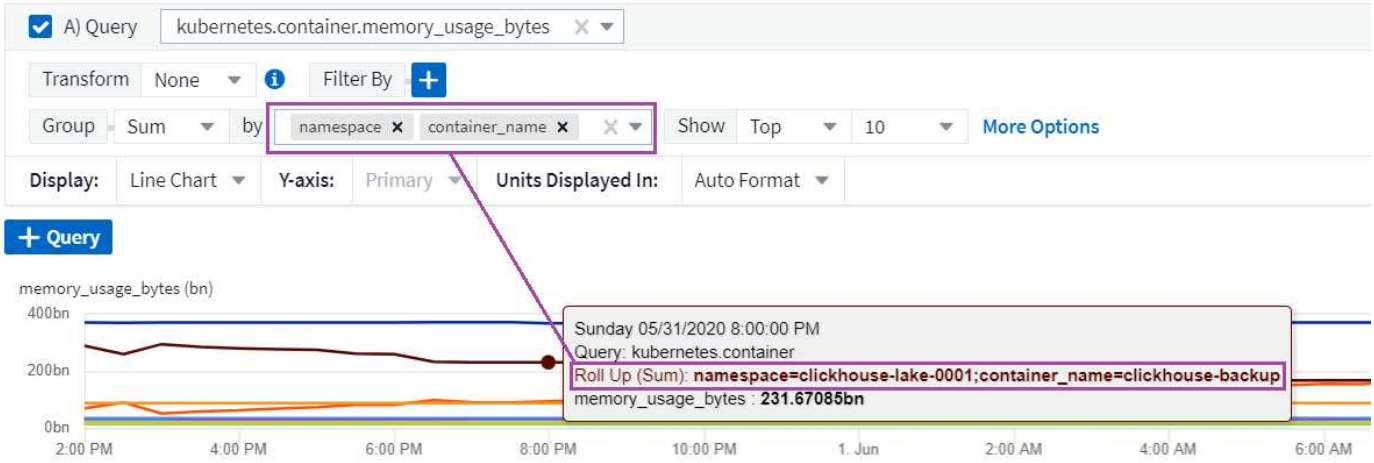
Sono stati apportati i seguenti miglioramenti ai widget della dashboard. Questi miglioramenti sono considerati funzionalità di anteprima e potrebbero non essere disponibili per tutti gli ambienti Cloud Insights .

- Nuovo selettore di oggetti/metriche: gli oggetti (archiviazione, disco, porte, nodi, ecc.) e le relative metriche (IOPS, latenza, conteggio CPU, ecc.) sono ora disponibili nei widget in un unico menu a discesa inclusivo con potenti funzionalità di ricerca. È possibile immettere più termini parziali nel menu a discesa e Cloud

Insights elencherà tutte le metriche degli oggetti che soddisfano tali termini.



- Raggruppamento di più tag: quando si lavora con dati di integrazione (Kubernetes, ecc.), è possibile raggruppare i dati in base a più tag/attributi. Ad esempio, somma l'utilizzo della memoria in base allo spazio dei nomi Kubernetes e al nome del contenitore.



Maggio 2020

Segnalazione dei ruoli utente

Sono stati aggiunti i seguenti ruoli per la segnalazione:

- Cloud Insights Consumers: possono eseguire e visualizzare report
- Autori di Cloud Insights : possono eseguire le funzioni Consumer, nonché creare e gestire report e dashboard

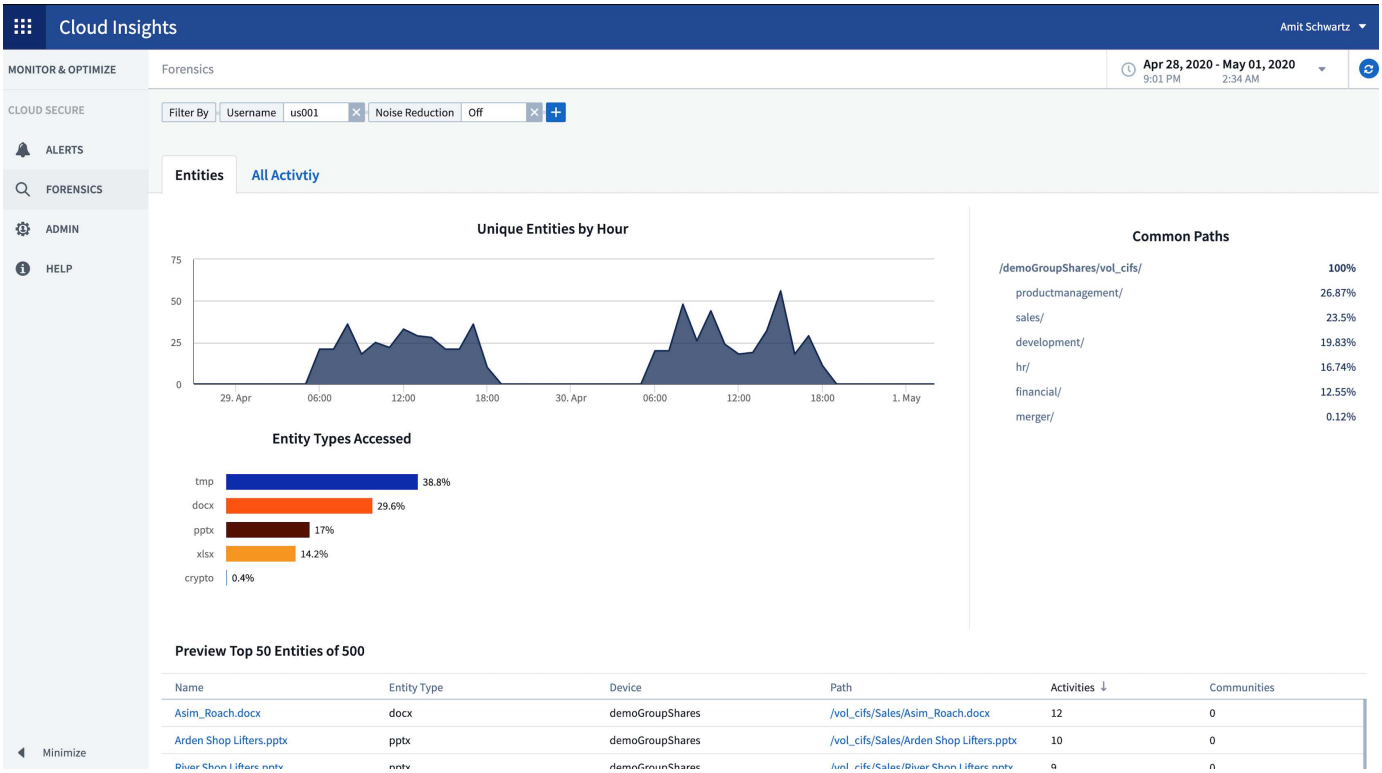
- Amministratori di Cloud Insights : possono eseguire le funzioni di autore e tutte le attività amministrative

Aggiornamenti Cloud Secure

Cloud Insights include le seguenti recenti modifiche a Cloud Secure .

Nella pagina Forensics > Activity Forensics, forniamo due visualizzazioni per analizzare e indagare l'attività degli utenti:

- Visualizzazione attività, focalizzata sull'attività dell'utente (Quale operazione? Dove è stato eseguito?)
- Visualizzazione delle entità, incentrata sui file a cui l'utente ha avuto accesso.

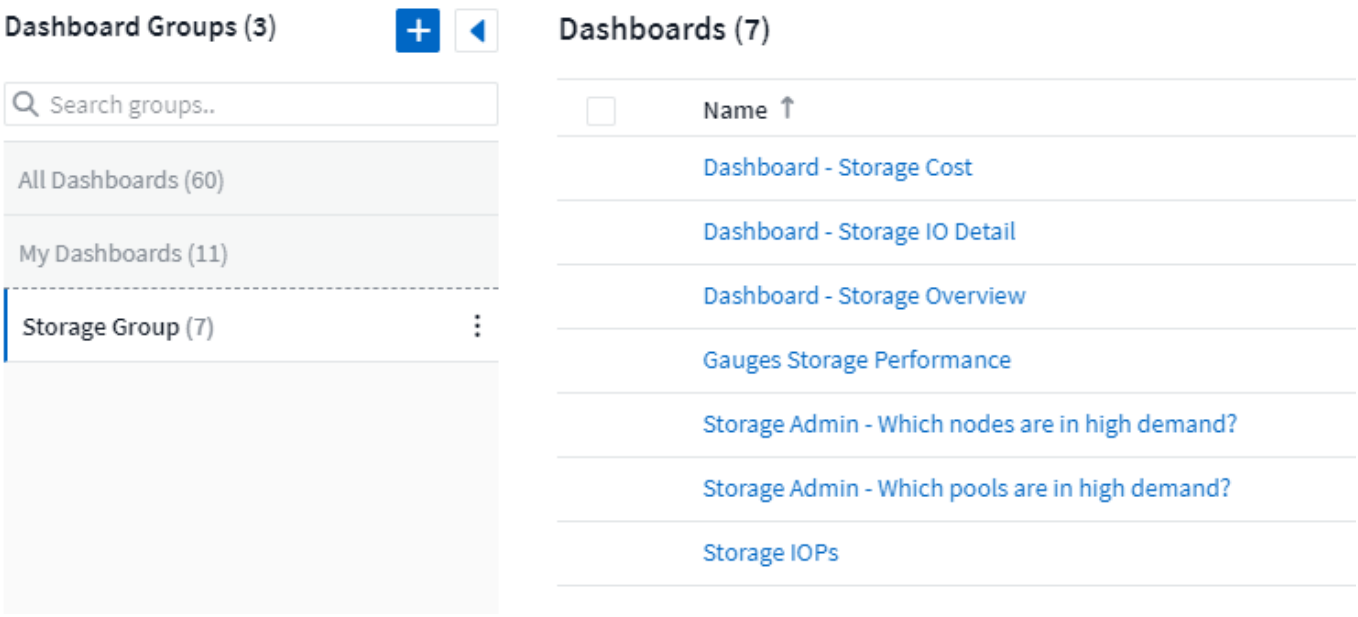


Inoltre, la notifica e-mail di avviso ora contiene un collegamento diretto alla pagina di avviso.

Raggruppamento della dashboard

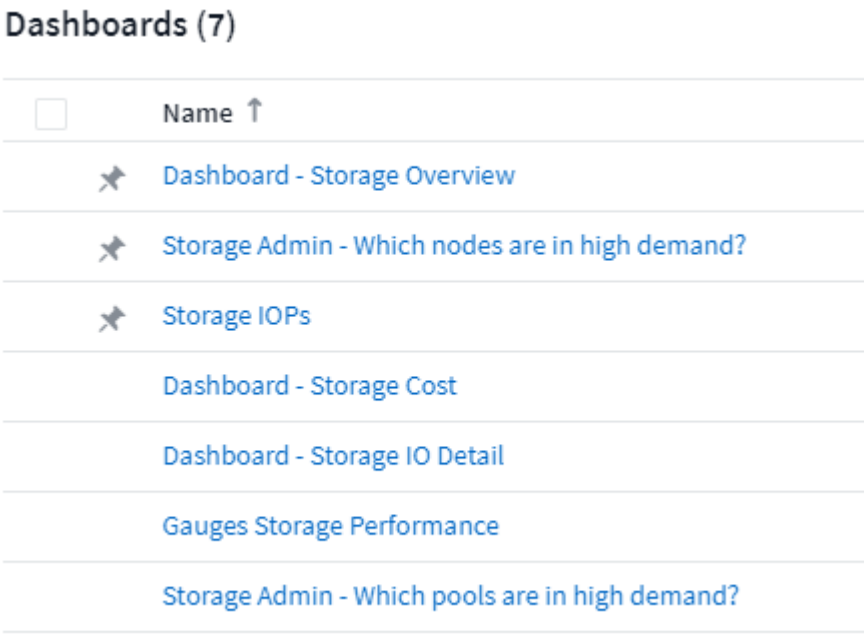
Il raggruppamento della dashboard consente una migliore"gestione dei cruscotti" che sono rilevanti per te. È possibile aggiungere dashboard correlate a un gruppo per una gestione "unificata", ad esempio, dello storage o delle macchine virtuali.

I gruppi sono personalizzati per utente, quindi i gruppi di una persona possono essere diversi da quelli di un'altra. Puoi avere tutti i gruppi di cui hai bisogno, con poche o tante dashboard in ogni gruppo, a seconda delle tue esigenze.



Fissaggio della dashboard

È possibile aggiungere dashboard in modo che i preferiti vengano sempre visualizzati in cima all'elenco.



Modalità TV e aggiornamento automatico

"Modalità TV e aggiornamento automatico"consentono la visualizzazione dei dati in tempo quasi reale su una dashboard o una pagina di risorse:

- La **Modalità TV** offre una visualizzazione ordinata; il menu di navigazione è nascosto, lasciando più spazio sullo schermo per la visualizzazione dei dati.
- I dati nei widget sulle dashboard e nelle landing page delle risorse vengono **aggiornati automaticamente** in base a un intervallo di aggiornamento (anche solo ogni 10 secondi) determinato dall'intervallo di tempo

della dashboard selezionato (o dall'intervallo di tempo del widget, se impostato per sovrascrivere l'orario della dashboard).

La modalità TV e l'aggiornamento automatico, combinati, offrono una visualizzazione in tempo reale dei dati di Cloud Insights , perfetti per dimostrazioni fluide o per il monitoraggio interno.

Aprile 2020

Nuove scelte di intervallo di tempo della dashboard

Le scelte di intervallo di tempo per le dashboard e altre pagine di Cloud Insights ora includono *Ultima ora* e *Ultimi 15 minuti*.

Aggiornamenti Cloud Secure

Cloud Insights include le seguenti recenti modifiche a Cloud Secure .

- Miglior riconoscimento delle modifiche ai metadati di file e cartelle per rilevare se l'utente ha modificato l'autorizzazione, il proprietario o la proprietà del gruppo.
- Esporta il report sulle attività degli utenti in formato CSV.

Cloud Secure monitora e verifica tutte le operazioni di accesso degli utenti a file e cartelle. L'audit delle attività consente di rispettare le policy di sicurezza interne, soddisfare i requisiti di conformità esterni quali PCI, GDPR e HIPAA e condurre indagini su violazioni dei dati e incidenti di sicurezza.

Ora predefinita della dashboard

L'intervallo di tempo predefinito per le dashboard è ora di 3 ore anziché 24 ore.

Tempi di aggregazione ottimizzati

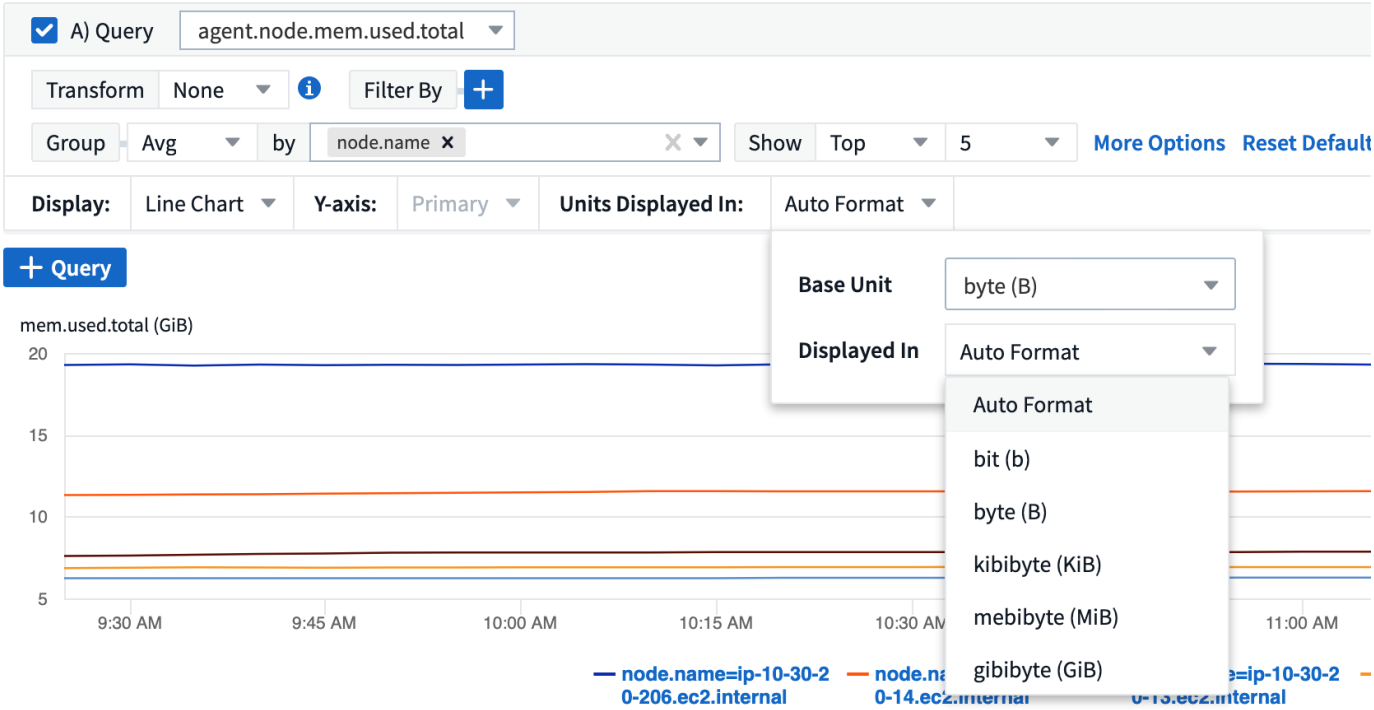
Ottimizzato"aggregazione temporale" gli intervalli nei widget delle serie temporali (grafici a linee, spline, ad area e ad area impilata) sono più frequenti per gli intervalli di tempo di 3 e 24 ore del dashboard/widget, consentendo una rappresentazione più rapida dei dati.

- L'intervallo di tempo di 3 ore si ottimizza con un intervallo di aggregazione di 1 minuto. In precedenza erano 5 minuti.
- L'intervallo di tempo di 24 ore si ottimizza in un intervallo di aggregazione di 30 minuti. In precedenza era di 1 ora.

È comunque possibile ignorare l'aggregazione ottimizzata impostando un intervallo personalizzato.

Formato automatico dell'unità di visualizzazione

Nella maggior parte dei widget, Cloud Insights conosce l'unità di base in cui visualizzare i valori, ad esempio *Megabyte*, *Migliaia*, *Percentuale*, *Millisecondi (ms)*, ecc., e ora"formatta automaticamente" il widget all'unità più leggibile. Ad esempio, un valore di dati pari a 1.234.567.890 byte verrebbe formattato automaticamente in 1,23 gibibyte. In molti casi, Cloud Insights conosce il formato migliore per i dati acquisiti. Nei casi in cui non si conosce il formato migliore o nei widget in cui si desidera ignorare la formattazione automatica, è possibile scegliere il formato desiderato.

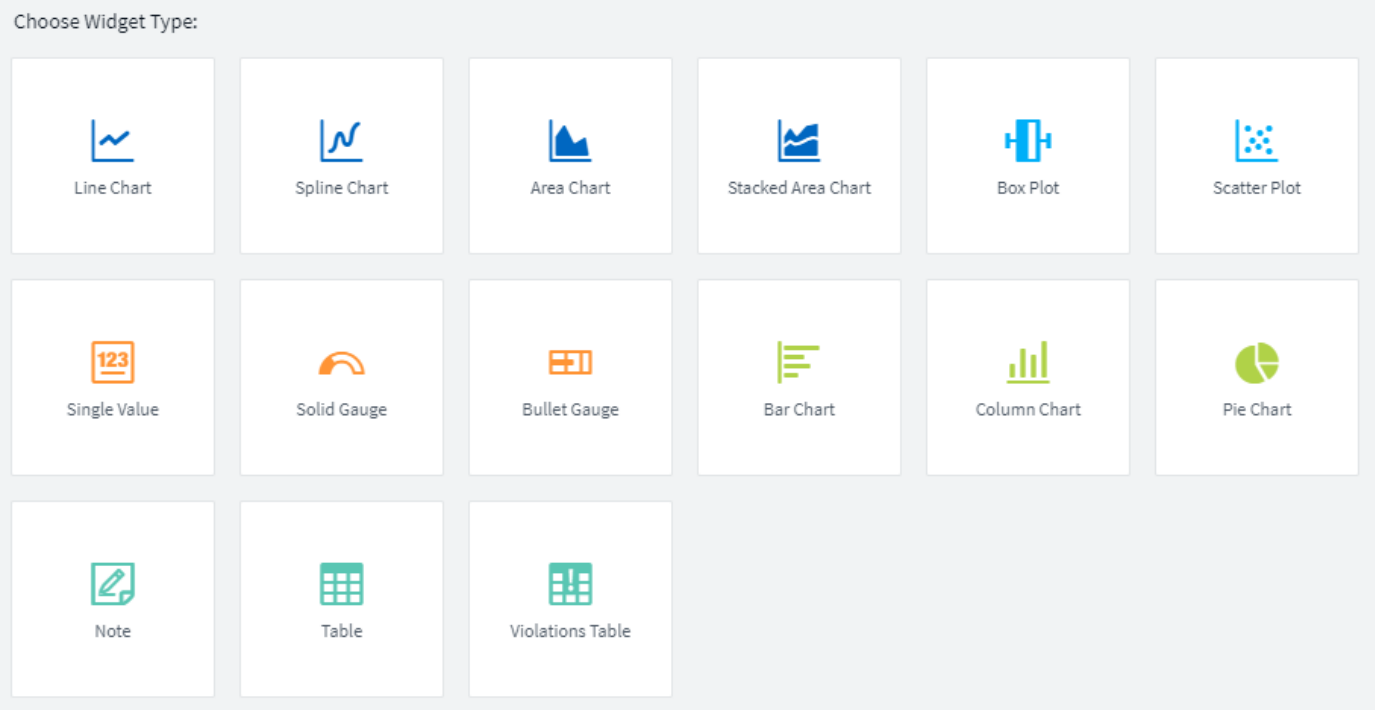


Importa annotazioni tramite API

Con la potente API di Cloud Insights Premium Edition, ora puoi"importa annotazioni" e assegnarli agli oggetti utilizzando un file .CSV. È anche possibile importare applicazioni e assegnare entità aziendali nello stesso modo.

Selettore widget più semplice

Aggiungere widget a dashboard e landing page di asset è più semplice grazie a un nuovo selettore di widget che mostra tutti i tipi di widget in un'unica vista, così l'utente non deve più scorrere un elenco di tipi di widget per trovare quello che desidera aggiungere. I widget correlati sono coordinati per colore e raggruppati per prossimità nel nuovo selettore.



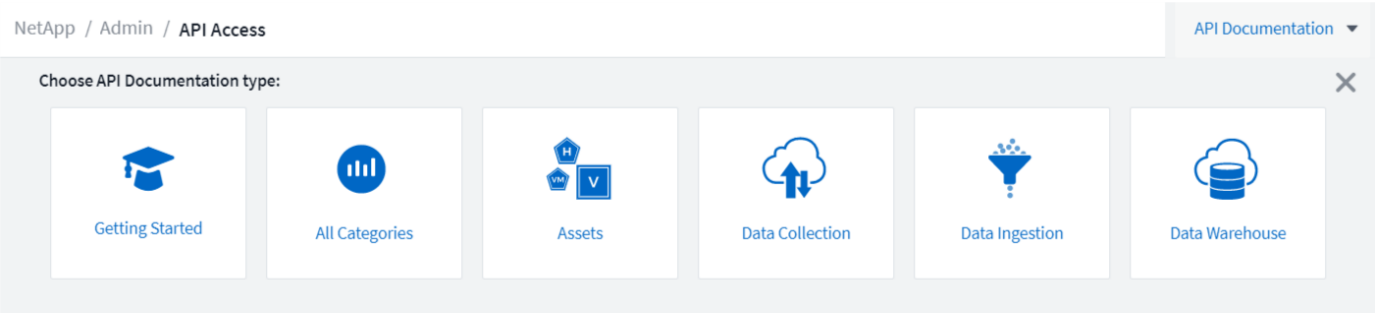
Febbraio 2020

API con edizione Premium

Cloud Insights Premium Edition è dotato di un"potente API" che può essere utilizzato per integrare Cloud Insights con altre applicazioni, come CMDB o altri sistemi di ticketing.

Informazioni dettagliate basate su Swagger sono disponibili in **Amministrazione > Accesso API**, sotto il link **Documentazione API**. Swagger fornisce una breve descrizione e informazioni sull'utilizzo dell'API e ti consente di provare ciascuna API nel tuo ambiente.

L'API Cloud Insights utilizza i token di accesso per fornire un accesso basato su autorizzazioni a categorie di API, come ASSET o COLLECTION.



Polling iniziale dopo l'aggiunta di un raccoglitore dati

In precedenza, dopo aver configurato un nuovo raccoglitore dati, Cloud Insights interrogava immediatamente il raccoglitore dati per raccogliere i dati di inventario, ma attendeva l'intervallo di interrogazione delle prestazioni configurato (in genere 15 minuti) per raccogliere i dati iniziali sulle prestazioni. Attenderebbe quindi un altro

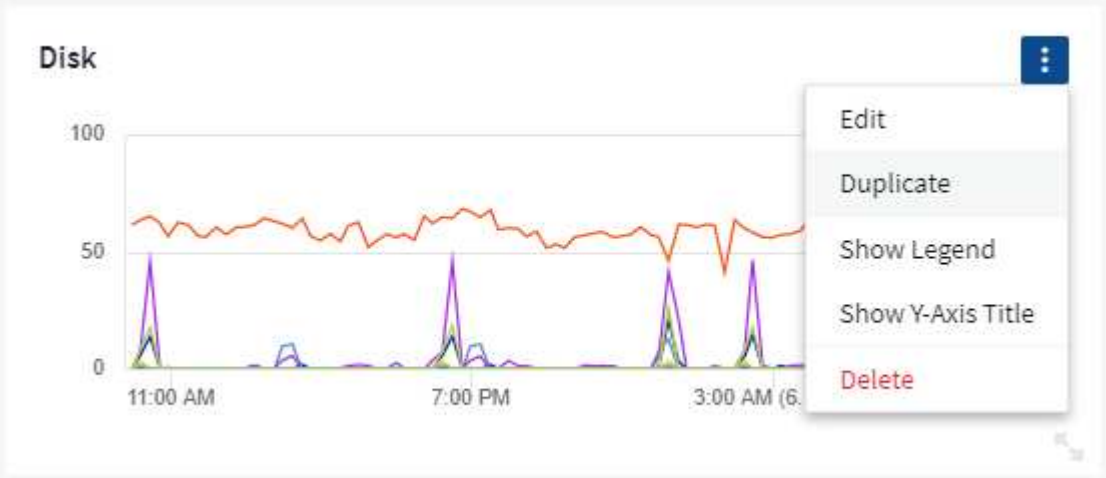
intervallo prima di avviare il secondo sondaggio sulle prestazioni, il che significa che ci vorrebbero fino a *30 minuti* prima che dati significativi venissero acquisiti da un nuovo raccoglitore di dati.

Raccoglitore di dati"sondaggi" è stato notevolmente migliorato, in modo che il sondaggio iniziale sulle prestazioni venga eseguito subito dopo il sondaggio sull'inventario, mentre il secondo sondaggio sulle prestazioni venga eseguito entro pochi secondi dal completamento del primo sondaggio sulle prestazioni. Ciò consente a Cloud Insights di iniziare a mostrare dati utili su dashboard e grafici in tempi molto brevi.

Questo comportamento di sondaggio si verifica anche dopo aver modificato la configurazione di un raccoglitore dati esistente.

Duplicazione dei widget più semplice

Creare una copia di un widget su una dashboard o una landing page è più facile che mai. Nella modalità di modifica della dashboard, fare clic sul menu sul widget e selezionare **Duplica**. Viene avviato l'editor dei widget, precompilato con la configurazione del widget originale e con un suffisso "copia" nel nome del widget. Puoi apportare facilmente tutte le modifiche necessarie e salvare il nuovo widget. Il widget verrà posizionato nella parte inferiore della dashboard e potrai posizionarlo come preferisci. Ricordati di salvare la dashboard una volta completate tutte le modifiche.



Accesso singolo (SSO)

Con Cloud Insights Premium Edition, gli amministratori possono abilitare *"Accesso unico" * Accesso (SSO) a Cloud Insights per tutti gli utenti del dominio aziendale, senza doverli invitare individualmente. Con l'SSO abilitato, qualsiasi utente con lo stesso indirizzo email di dominio può accedere a Cloud Insights utilizzando le proprie credenziali aziendali.

SSO è disponibile solo in Cloud Insights Premium Edition e deve essere configurato prima di poter essere abilitato per Cloud Insights. La configurazione SSO include"Federazione di identità" tramite NetApp Cloud Central. La federazione consente agli utenti con accesso Single Sign-On di accedere ai tuoi account NetApp Cloud Central utilizzando le credenziali della tua directory aziendale.

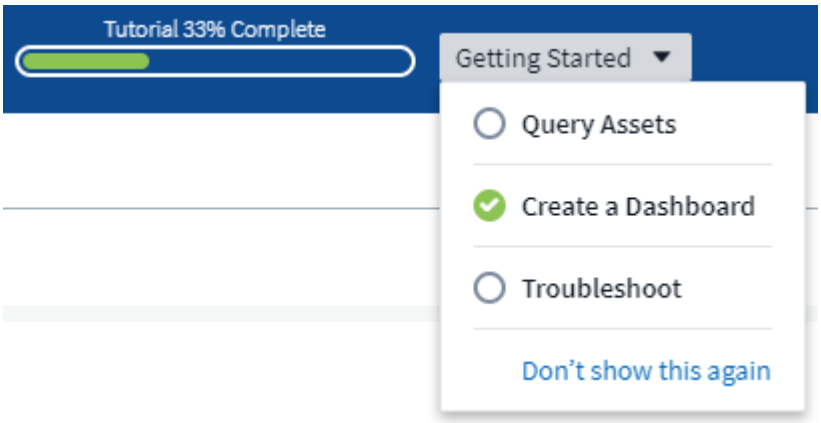
Gennaio 2020

Documentazione Swagger per REST API

Swagger spiega ogni API REST disponibile in Cloud Insights, nonché il suo utilizzo e la sua sintassi. Le informazioni sulle API Cloud Insights sono disponibili in"documentazione" .

Barra di avanzamento dei tutorial sulle funzionalità

L'elenco di controllo dei tutorial sulle funzionalità è stato spostato nel banner superiore e ora presenta un indicatore di avanzamento. I tutorial sono disponibili per ogni utente fino alla loro chiusura e sono sempre disponibili in Cloud Insights"documentazione" .



Modifiche all'unità di acquisizione

Quando si installa un'unità di acquisizione (AU) su un host o una VM che ha lo stesso nome di un'AU già installata, Cloud Insights garantisce un nome univoco aggiungendo al nome dell'AU "_1", "_2" e così via. Questo vale anche quando si disinstalla e si reinstalla un'AU dalla stessa VM senza prima rimuoverla da Cloud Insights. Vuoi un nome AU completamente diverso? Nessun problema: le AU possono essere rinominate dopo l'installazione.

Aggregazione temporale ottimizzata nei widget

Nei widget puoi scegliere tra un intervallo di aggregazione temporale *Ottimizzato* o un intervallo *Personalizzato* da te impostato. L'aggregazione ottimizzata seleziona automaticamente l'intervallo di tempo corretto in base all'intervallo di tempo della dashboard selezionato (o all'intervallo di tempo del widget, se si sovrascrive l'orario della dashboard). L'intervallo cambia dinamicamente man mano che cambia l'intervallo di tempo della dashboard o del widget.

Procedura semplificata "Introduzione a Cloud Insights"

La procedura per iniziare a utilizzare Cloud Insights è stata semplificata per rendere la configurazione iniziale più semplice e agevole. Basta selezionare un raccoglitore di dati iniziale e seguire le istruzioni. Cloud Insights ti guiderà nella configurazione del raccoglitore dati e di qualsiasi agente o unità di acquisizione richiesta. Nella maggior parte dei casi importerà anche una o più dashboard iniziali, così potrai iniziare ad acquisire rapidamente informazioni sul tuo ambiente (ma tieni presente che Cloud Insights potrebbe impiegare fino a 30 minuti per raccogliere dati significativi).

Ulteriori miglioramenti:

- L'installazione dell'unità di acquisizione è più semplice e veloce.

- Le scelte dei raccoglitori di dati in ordine alfabetico semplificano la ricerca di quello che stai cercando.
- Le istruzioni di configurazione migliorate di Data Collector sono più facili da seguire.
- Gli utenti esperti possono saltare la procedura di avvio con un semplice clic.
- Una nuova barra di avanzamento ti mostra a che punto sei nel processo.

Onboarding Data Infrastructure Insights

Prima di poter iniziare a lavorare con Data Infrastructure Insights, è necessario registrarsi sul portale * NetApp Console*. Se disponi già di un accesso NetApp Console , puoi iniziare una prova gratuita di Data Infrastructure Insights con pochi rapidi passaggi.

Queste istruzioni sono in fase di aggiornamento. Controlla di nuovo più tardi.

Sicurezza

Data Infrastructure Insights

Per NetApp la sicurezza dei dati dei prodotti e dei clienti è di fondamentale importanza. Data Infrastructure Insights segue le migliori pratiche di sicurezza durante l'intero ciclo di vita del rilascio per garantire che i dati e le informazioni dei clienti siano protetti nel miglior modo possibile.

Panoramica sulla sicurezza

Sicurezza fisica

L'infrastruttura di produzione Data Infrastructure Insights è ospitata in Amazon Web Services (AWS). I controlli relativi alla sicurezza fisica e ambientale per i server di produzione Data Infrastructure Insights , che includono edifici e serrature o chiavi utilizzate sulle porte, sono gestiti da AWS. Secondo AWS: "L'accesso fisico è controllato sia sul perimetro che nei punti di ingresso dell'edificio da personale di sicurezza professionale che utilizza videosorveglianza, sistemi di rilevamento delle intrusioni e altri mezzi elettronici. Il personale autorizzato utilizza meccanismi di autenticazione a più fattori per accedere ai piani del data center."

Data Infrastructure Insights segue le migliori pratiche del"Modello di responsabilità condivisa" descritto da AWS.

Sicurezza del prodotto

Data Infrastructure Insights segue un ciclo di sviluppo in linea con i principi Agile, consentendoci così di affrontare più rapidamente eventuali difetti software legati alla sicurezza, rispetto alle metodologie di sviluppo con cicli di rilascio più lunghi. Utilizzando metodologie di integrazione continua, siamo in grado di rispondere rapidamente ai cambiamenti sia funzionali che di sicurezza. Le procedure e le policy di gestione del cambiamento definiscono quando e come si verificano i cambiamenti e contribuiscono a mantenere la stabilità dell'ambiente di produzione. Tutte le modifiche significative vengono comunicate formalmente, coordinate, opportunamente esaminate e approvate prima di essere rilasciate nell'ambiente di produzione.

Sicurezza di rete

L'accesso di rete alle risorse nell'ambiente Data Infrastructure Insights è controllato da firewall basati su host. Ogni risorsa (ad esempio un bilanciatore del carico o un'istanza di macchina virtuale) dispone di un firewall basato su host che limita il traffico in entrata solo alle porte necessarie affinché la risorsa svolga la sua funzione.

Data Infrastructure Insights utilizza vari meccanismi, tra cui servizi di rilevamento delle intrusioni, per monitorare l'ambiente di produzione alla ricerca di anomalie di sicurezza.

Valutazione del rischio

Il team di Data Infrastructure Insights segue un processo formalizzato di valutazione del rischio per fornire un metodo sistematico e ripetibile per identificare e valutare i rischi, in modo che possano essere gestiti in modo appropriato tramite un piano di trattamento del rischio.

Protezione dei dati

L'ambiente di produzione Data Infrastructure Insights è configurato in un'infrastruttura altamente ridondante che utilizza più zone di disponibilità per tutti i servizi e i componenti. Oltre a utilizzare un'infrastruttura di elaborazione altamente disponibile e ridondante, i dati critici vengono sottoposti a backup a intervalli regolari e i ripristini vengono testati periodicamente. Le policy e le procedure di backup formali riducono al minimo l'impatto delle interruzioni delle attività aziendali e proteggono i processi aziendali dagli effetti di guasti dei sistemi informativi o disastri, garantendone la ripresa tempestiva e adeguata.

Autenticazione e gestione degli accessi

L'accesso dei clienti a Data Infrastructure Insights avviene tramite interazioni con l'interfaccia utente del browser tramite https. L'autenticazione viene effettuata tramite il servizio di terze parti Auth0. NetApp ha scelto questo come livello di autenticazione per tutti i servizi Cloud Data.

Data Infrastructure Insights segue le best practice del settore, tra cui "Privilegio minimo" e "Controllo degli accessi basato sui ruoli" per l'accesso logico all'ambiente di produzione di Data Infrastructure Insights . L'accesso è controllato in base alla stretta necessità e viene concesso solo a personale autorizzato selezionato mediante meccanismi di autenticazione a più fattori.

Raccolta e protezione dei dati dei clienti

Tutti i dati dei clienti vengono crittografati durante il transito sulle reti pubbliche e crittografati a riposo. Data Infrastructure Insights utilizza la crittografia in vari punti del sistema per proteggere i dati dei clienti tramite tecnologie che includono Transport Layer Security (TLS) e l'algoritmo standard del settore AES-256.

Deprovisioning del cliente

Le notifiche e-mail vengono inviate a intervalli diversi per informare il cliente che il suo abbonamento sta per scadere. Una volta scaduto l'abbonamento, l'interfaccia utente viene limitata e inizia un periodo di tolleranza per la raccolta dei dati. Il cliente viene quindi avvisato tramite e-mail. Gli abbonamenti di prova hanno un periodo di grazia di 14 giorni, mentre gli abbonamenti a pagamento hanno un periodo di grazia di 28 giorni. Una volta scaduto il periodo di tolleranza, il cliente verrà avvisato tramite e-mail che l'account verrà eliminato entro 2 giorni. Anche un cliente pagante può richiedere direttamente di uscire dal servizio.

I tenant scaduti e tutti i dati dei clienti associati vengono eliminati dal team Data Infrastructure Insights Operations (SRE) al termine del periodo di tolleranza o alla conferma della richiesta del cliente di chiudere il proprio account. In entrambi i casi, il team SRE esegue una chiamata API per eliminare l'account. La chiamata API elimina l'istanza del tenant e tutti i dati del cliente. L'eliminazione del cliente viene verificata chiamando la stessa API e verificando che lo stato del tenant del cliente sia "ELIMINATO".

Gestione degli incidenti di sicurezza

Data Infrastructure Insights è integrato con il processo Product Security Incident Response Team (PSIRT) di NetApp per individuare, valutare e risolvere le vulnerabilità note. PSIRT acquisisce informazioni sulle vulnerabilità da più canali, tra cui segnalazioni dei clienti, ingegneria interna e fonti ampiamente riconosciute come il database CVE.

Se il team di ingegneria Data Infrastructure Insights rileva un problema, avvierà il processo PSIRT, valuterà e potenzialmente risolverà il problema.

È anche possibile che un cliente o un ricercatore Data Infrastructure Insights identifichi un problema di sicurezza con il prodotto Data Infrastructure Insights e segnali il problema al supporto tecnico o direttamente al team di risposta agli incidenti di NetApp. In questi casi, il team Data Infrastructure Insights avvierà il processo PSIRT, valuterà e potenzialmente risolverà il problema.

Test di vulnerabilità e penetrazione

Data Infrastructure Insights segue le migliori pratiche del settore ed esegue regolarmente test di vulnerabilità e penetrazione avvalendosi di professionisti e aziende della sicurezza interne ed esterne.

Formazione sulla consapevolezza della sicurezza

Tutto il personale di Data Infrastructure Insights segue una formazione sulla sicurezza, sviluppata per i singoli ruoli, per garantire che ogni dipendente sia in grado di gestire le sfide specifiche in materia di sicurezza dei propri ruoli.

Conformità

Data Infrastructure Insights esegue audit indipendenti di terze parti e convalide da parte di società di revisione contabile autorizzate esterne sulla sua sicurezza, sui suoi processi e sui suoi servizi, incluso il completamento dell'audit SOC 2.

Avvisi di sicurezza NetApp

Puoi visualizzare gli avvisi di sicurezza disponibili di NetApp"Qui" .

Informazioni e Regione

NetApp prende molto seriamente la sicurezza delle informazioni dei clienti. Ecco come e dove Data Infrastructure Insights archivia le tue informazioni.

Quali informazioni memorizza Data Infrastructure Insights ?

Data Infrastructure Insights memorizza le seguenti informazioni:

- Dati sulle prestazioni

  I dati sulle prestazioni sono dati di serie temporali che forniscono informazioni sulle prestazioni del dispositivo/sorgente monitorato. Ciò include, ad esempio, il numero di I/O forniti da un sistema di archiviazione, la capacità di elaborazione di una porta FibreChannel, il numero di pagine fornite da un server Web, il tempo di risposta di un database e altro ancora.

- dati di inventario

  I dati di inventario sono costituiti da metadati che descrivono il dispositivo/la sorgente monitorati e la loro configurazione. Ciò include, ad esempio, le versioni hardware e software installate, i dischi e le LUN in un sistema di archiviazione, i core della CPU, la RAM e i dischi di una macchina virtuale, gli spazi tabella di un database, il numero e il tipo di porte su uno switch SAN, i nomi di directory/file (se Storage Workload Security è abilitato), ecc.

- Dati di configurazione

  Riepiloga i dati di configurazione forniti dal cliente, utilizzati per gestire l'inventario e le operazioni del cliente, ad esempio nomi host o indirizzi IP dei dispositivi monitorati, intervalli di polling, valori di timeout, ecc.

- Segreti

  I segreti sono costituiti dalle credenziali utilizzate dalla Data Infrastructure Insights Acquisition Unit per

accedere ai dispositivi e ai servizi dei clienti. Queste credenziali vengono crittografate utilizzando una crittografia asimmetrica avanzata e le chiavi private vengono memorizzate solo sulle unità di acquisizione e non escono mai dall'ambiente del cliente. A causa di questa progettazione, anche gli SRE Data Infrastructure Insights privilegiati non sono in grado di accedere ai segreti dei clienti in testo normale.

- Dati funzionali

  Si tratta di dati generati in seguito alla fornitura del Cloud Data Service da parte di NetApp , che informano NetApp sullo sviluppo, l'implementazione, le operazioni, la manutenzione e la protezione del Cloud Data Service. I dati funzionali non contengono informazioni sul cliente o informazioni personali.

- Dati di accesso dell'utente

  Informazioni di autenticazione e accesso che consentono a NetApp Console di comunicare con i siti Data Infrastructure Insights regionali, inclusi i dati relativi all'autorizzazione dell'utente.

- Dati della directory utente della sicurezza del carico di lavoro di archiviazione

  Nei casi in cui la funzionalità Workload Security è abilitata E il cliente sceglie di abilitare il raccoglitore di directory utente, il sistema memorizzerà i nomi visualizzati degli utenti, gli indirizzi e-mail aziendali e altre informazioni raccolte da Active Directory.

> I dati della directory utente si riferiscono alle informazioni della directory utente raccolte dal raccoglitore dati della directory utente di Workload Security, non ai dati sugli utenti stessi di Data Infrastructure Insights/Workload Security.

Nessun dato personale esplicito viene raccolto dalle risorse infrastrutturali e dei servizi. Le informazioni raccolte sono costituite solo da parametri di prestazione, informazioni di configurazione e metadati dell'infrastruttura, in modo molto simile a quanto avviene con i servizi telefonici di molti fornitori, tra cui il supporto automatico NetApp e ActiveIQ. Tuttavia, a seconda delle convenzioni di denominazione del cliente, i dati per condivisioni, volumi, VM, qtree, applicazioni, ecc. possono contenere informazioni di identificazione personale.

Se Workload Security è abilitato, il sistema esamina anche i nomi di file e directory su SMB o altre condivisioni, che potrebbero contenere informazioni personali identificabili. Quando i clienti abilitano Workload Security User Directory Collector (che sostanzialmente mappa i SID di Windows ai nomi utente tramite Active Directory), il nome visualizzato, l'indirizzo e-mail aziendale e tutti gli attributi aggiuntivi selezionati verranno raccolti e archiviati da Data Infrastructure Insights.

Inoltre, vengono conservati i registri di accesso a Data Infrastructure Insights , che contengono gli indirizzi IP e gli indirizzi e-mail degli utenti utilizzati per accedere al servizio.

Dove vengono archiviate le mie informazioni?

Data Infrastructure Insights archivia le informazioni in base alla regione in cui è stato creato l'ambiente.

Nella regione host vengono memorizzate le seguenti informazioni:

- Telemetria e informazioni su asset/oggetti, inclusi contatori e metriche delle prestazioni
- Informazioni sull'unità di acquisizione
- Dati funzionali
- Informazioni di audit sulle attività degli utenti all'interno di Data Infrastructure Insights

- Informazioni sulla sicurezza del carico di lavoro di Active Directory
- Informazioni sull'audit di sicurezza del carico di lavoro

Le seguenti informazioni risiedono negli Stati Uniti, indipendentemente dalla regione che ospita l'ambiente Data Infrastructure Insights :

- Informazioni sul sito ambientale (talvolta denominato "inquilino"), come il proprietario del sito/account.
- Informazioni che consentono a NetApp Console di comunicare con i siti Data Infrastructure Insights regionali, incluso tutto ciò che riguarda l'autorizzazione dell'utente.
- Informazioni relative alla relazione tra l'utente Data Infrastructure Insights e il tenant.

Regioni ospitanti

Le regioni ospitanti includono:

- Stati Uniti: us-east-1
- EMEA: eu-central-1
- APAC: ap-southeast-2

Ulteriori informazioni

Per maggiori informazioni sulla privacy e la sicurezza di NetApp, consulta i seguenti xref:./* "Centro di fiducia"
* "Trasferimenti transfrontalieri di dati"
* "Regole aziendali vincolanti"
* "Rispondere alle richieste di dati di terze parti"
* "Principi sulla privacy NetApp"

Strumento SecurityAdmin

Data Infrastructure Insights include funzionalità di sicurezza che consentono al tuo ambiente di funzionare con maggiore sicurezza. Le funzionalità includono miglioramenti alla crittografia, all'hashing delle password e alla possibilità di modificare le password utente interne, nonché coppie di chiavi che crittografano e decrittografano le password.

Per proteggere i dati sensibili, NetApp consiglia di modificare le chiavi predefinite e la password utente *Acquisition* dopo un'installazione o un aggiornamento.

Le password crittografate dell'origine dati vengono archiviate in Data Infrastructure Insights, che utilizza una chiave pubblica per crittografare le password quando un utente le immette in una pagina di configurazione del raccoglitore dati. Data Infrastructure Insights non dispone delle chiavi private necessarie per decrittografare le password del data collector; solo le Acquisition Unit (AU) dispongono della chiave privata del data collector necessaria per decrittografare le password del data collector.

Considerazioni sull'aggiornamento e l'installazione

Se il sistema Insight contiene configurazioni di sicurezza non predefinite (ad esempio se sono state modificate le password), è necessario eseguire il backup delle configurazioni di sicurezza. L'installazione di un nuovo software o, in alcuni casi, l'aggiornamento del software, ripristina la configurazione di sicurezza predefinita del sistema. Quando il sistema torna alla configurazione predefinita, è necessario ripristinare la configurazione non predefinita affinché il sistema funzioni correttamente.

Gestione della sicurezza sull'unità di acquisizione

Lo strumento SecurityAdmin consente di gestire le opzioni di sicurezza per Data Infrastructure Insights e viene eseguito sul sistema dell'unità di acquisizione. La gestione della sicurezza include la gestione di chiavi e password, il salvataggio e il ripristino delle configurazioni di sicurezza create o il ripristino delle configurazioni alle impostazioni predefinite.

Prima di iniziare

- Per installare il software Acquisition Unit (che include lo strumento SecurityAdmin), è necessario disporre dei privilegi di amministratore sul sistema AU.
- Se in seguito sono presenti utenti non amministratori che dovranno accedere allo strumento SecurityAdmin, è necessario aggiungerli al gruppo *cisys*. Il gruppo *cisys* viene creato durante l'installazione di AU.

Dopo l'installazione di AU, lo strumento SecurityAdmin si trova sul sistema dell'unità di acquisizione in una di queste posizioni:

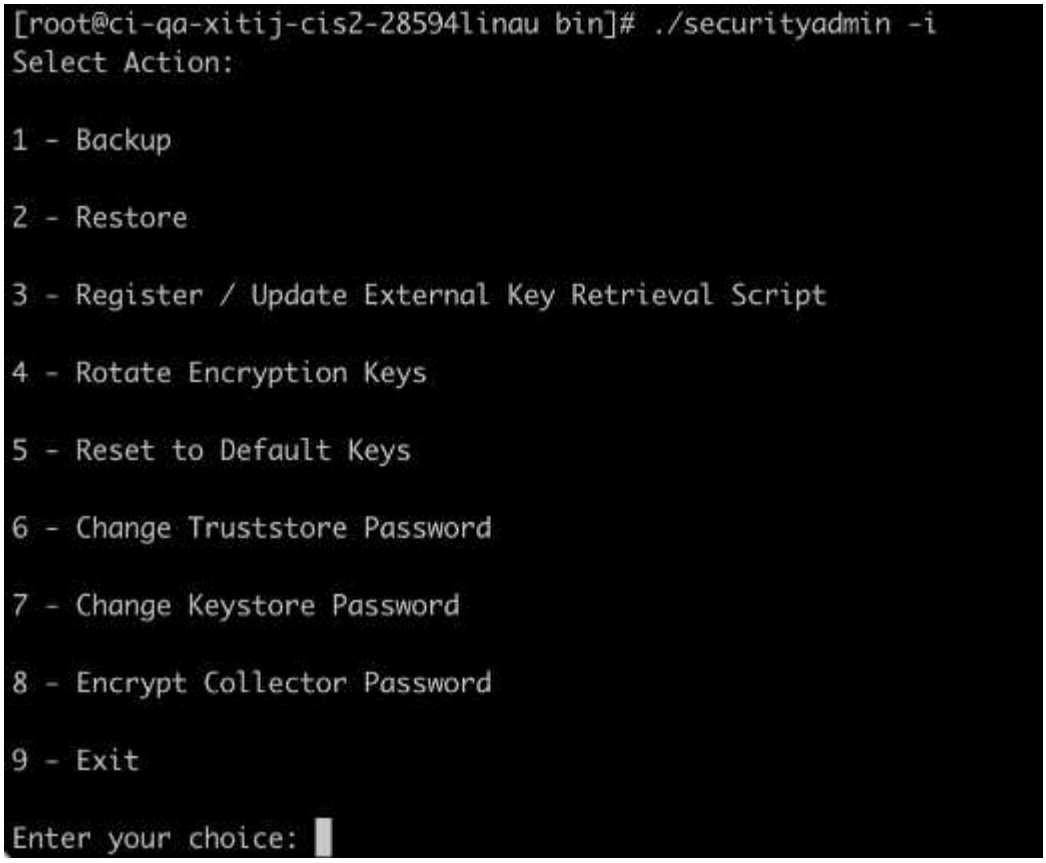
```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Utilizzo dello strumento SecurityAdmin

Avviare lo strumento SecurityAdmin in modalità interattiva (-i).

Si consiglia di utilizzare lo strumento SecurityAdmin in modalità interattiva, per evitare di passare segreti sulla riga di comando, che potrebbero essere catturati nei log.

Vengono visualizzate le seguenti opzioni:



1. **Backup**

   Crea un file zip di backup del vault contenente tutte le password e le chiavi e posiziona il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Si consiglia di mantenere sicuri i backup del vault, poiché contengono informazioni sensibili.

2. **Ripristinare**

   Ripristina il backup zip del vault creato. Una volta ripristinate, tutte le password e le chiavi vengono riportate ai valori esistenti al momento della creazione del backup.

   È possibile utilizzare Restore per sincronizzare password e chiavi su più server, ad esempio seguendo questi passaggi: 1) Modificare le chiavi di crittografia sull'AU. 2) Creare un backup del vault. 3) Ripristinare il backup del vault su ciascuna delle AU.

3. **Registra/Aggiorna lo script di recupero delle chiavi esterne**

   Utilizzare uno script esterno per registrare o modificare le chiavi di crittografia AU utilizzate per crittografare o decrittografare le password dei dispositivi.

   Quando si modificano le chiavi di crittografia, è opportuno eseguire il backup della nuova configurazione di sicurezza in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

Nota che questa opzione è disponibile solo su Linux.

Quando si utilizza uno script di recupero delle chiavi personalizzato con lo strumento SecurityAdmin, tenere presente quanto segue:

- L'algoritmo attualmente supportato è RSA con un minimo di 2048 bit.
- Lo script deve restituire le chiavi privata e pubblica in testo normale. Lo script non deve restituire chiavi private e pubbliche crittografate.
- Lo script dovrebbe restituire contenuti grezzi e codificati (solo formato PEM).
- Lo script esterno deve avere i permessi *execute*.

4. **Ruota le chiavi di crittografia**

   Ruota le chiavi di crittografia (annulla la registrazione delle chiavi correnti e registra nuove chiavi). Per utilizzare una chiave da un sistema di gestione delle chiavi esterno, è necessario specificare l'ID della chiave pubblica e l'ID della chiave privata.

5. **Ripristina i tasti predefiniti**

   Reimposta la password dell'utente di acquisizione e le chiavi di crittografia dell'utente di acquisizione ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

6. **Cambia password Truststore**

   Cambia la password del truststore.

7. **Cambia password archivio chiavi**

   Cambia la password del keystore.

8. **Crittografa la password del collezionista**

   Crittografa la password del raccoglitore dati.

9. **Uscita**

   Uscire dallo strumento SecurityAdmin.

Scegli l'opzione che vuoi configurare e segui le istruzioni.

Specificare un utente per eseguire lo strumento

Se ti trovi in un ambiente controllato e attento alla sicurezza, potresti non disporre del gruppo *cisys* ma potresti comunque voler consentire a utenti specifici di eseguire lo strumento SecurityAdmin.

È possibile ottenere questo risultato installando manualmente il software AU e specificando l'utente/gruppo per il quale si desidera l'accesso.

- Utilizzando l'API, scaricare il CI Installer sul sistema AU e decomprimerlo.
  - Sarà necessario un token di autorizzazione monouso. Consulta la documentazione API Swagger (*Admin > Accesso API* e seleziona il link *Documentazione API*) e trova la sezione API *GET /au/oneTimeToken*.
  - Una volta ottenuto il token, utilizza l'API *GET /au/installers/{platform}/{version}* per scaricare il file di

installazione. Sarà necessario fornire la piattaforma (Linux o Windows) e la versione del programma di installazione.

- Copiare il file di installazione scaricato sul sistema AU e decomprimerlo.
- Passare alla cartella contenente i file ed eseguire il programma di installazione come root, specificando l'utente e il gruppo:

```
./cloudinsights-install.sh <User> <Group>
```

Se l'utente e/o il gruppo specificato non esistono, verranno creati. L'utente avrà accesso allo strumento SecurityAdmin.

Aggiornamento o rimozione del proxy

Lo strumento SecurityAdmin può essere utilizzato per impostare o rimuovere le informazioni proxy per l'unità di acquisizione eseguendo lo strumento con il parametro *-pr*:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Ad esempio, per rimuovere il proxy, eseguire questo comando:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Dopo aver eseguito il comando, è necessario riavviare l'unità di
acquisizione.
```

Per aggiornare un proxy, il comando è

```
./securityadmin -pr -upr <arg>
```

Recupero della chiave esterna

Se si fornisce uno script shell UNIX, questo può essere eseguito dall'unità di acquisizione per recuperare la **chiave privata** e la **chiave pubblica** dal sistema di gestione delle chiavi.

Per recuperare la chiave, Data Infrastructure Insights eseguirà lo script, passando due parametri: *key id* e *key type*. *Key id* può essere utilizzato per identificare la chiave nel sistema di gestione delle chiavi. Il *tipo di chiave* è "pubblico" o "privato". Quando il tipo di chiave è "pubblico", lo script deve restituire la chiave pubblica. Quando il tipo di chiave è "privato", è necessario restituire la chiave privata.

Per inviare la chiave all'unità di acquisizione, lo script deve stamparla sull'output standard. Lo script deve stampare *solo* la chiave sull'output standard; nessun altro testo deve essere stampato sull'output standard. Una volta che la chiave richiesta viene stampata sull'output standard, lo script deve uscire con un codice di uscita pari a 0; qualsiasi altro codice di ritorno è considerato un errore.

Lo script deve essere registrato con l'unità di acquisizione tramite lo strumento SecurityAdmin, che eseguirà lo script insieme all'unità di acquisizione. Lo script deve avere i permessi di *lettura* ed *esecuzione* per l'utente root e "cisys". Se lo script shell viene modificato dopo la registrazione, lo script shell modificato deve essere nuovamente registrato nell'unità di acquisizione.

parametro di input: ID chiave	Identificatore chiave utilizzato per identificare la chiave nel sistema di gestione delle chiavi del cliente.
parametro di input: tipo di chiave	pubblico o privato.
produzione	La chiave richiesta deve essere stampata sull'output standard. Attualmente è supportata la chiave RSA a 2048 bit. Le chiavi devono essere codificate e stampate nel seguente formato: formato chiave privata: PEM, codificato DER PKCS8 PrivateKeyInfo RFC 5958 formato chiave pubblica: PEM, codificato DER X.509 SubjectPublicKeyInfo RFC 5280
codice di uscita	Codice di uscita zero in caso di successo. Tutti gli altri valori di uscita sono considerati fallimentari.
permessi di script	Lo script deve avere i permessi di lettura ed esecuzione per l'utente root e "cisys".
registri	Le esecuzioni degli script vengono registrate. I log possono essere trovati in - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Crittografia di una password per l'uso nell'API

L'opzione 8 consente di crittografare una password, che può poi essere passata a un raccoglitore di dati tramite API.

Avviare lo strumento SecurityAdmin in modalità interattiva e selezionare l'opzione 8: *Crittografa password*.

```
 securityadmin.sh -i
Ti verrà chiesto di inserire la password che desideri crittografare.
Tieni presente che i caratteri digitati non vengono visualizzati sullo
schermo.  Reinserire la password quando richiesto.
```

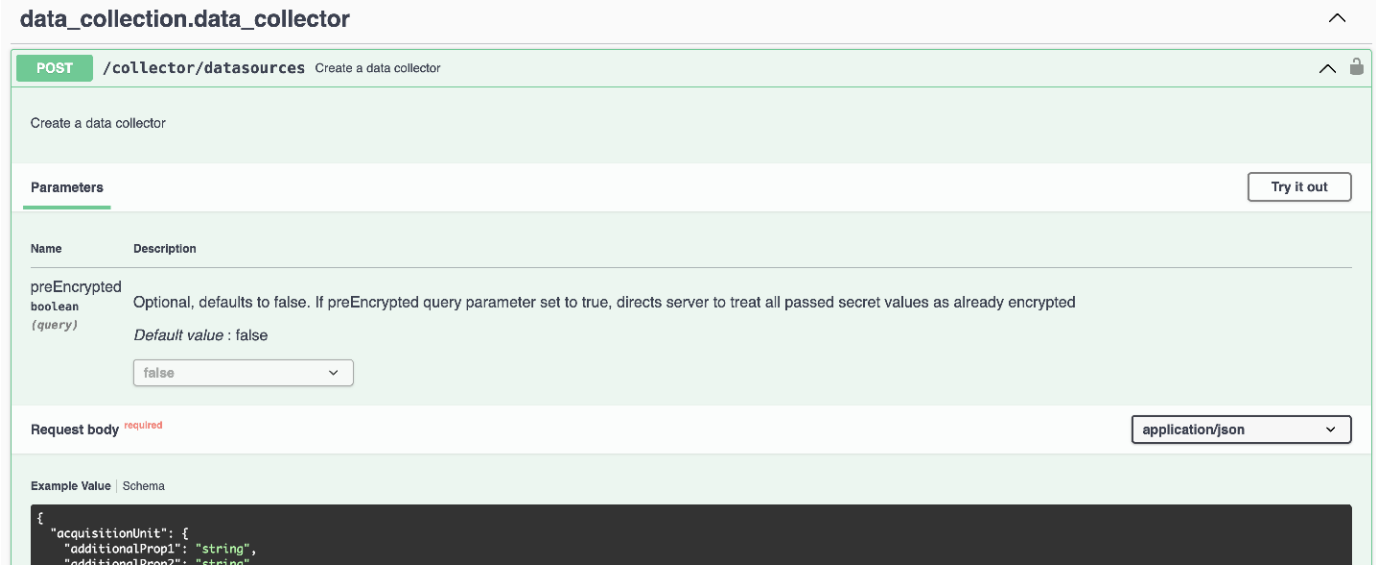
In alternativa, se si desidera utilizzare il comando in uno script, su una riga di comando utilizzare *securityadmin.sh* con il parametro "-enc", passando la password non crittografata:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Esempio CLI"]
```

La password crittografata viene visualizzata sullo schermo. Copia l'intera stringa, compresi eventuali simboli iniziali o finali.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

Per inviare la password crittografata a un raccoglitore di dati, è possibile utilizzare l'API di raccolta dati. È possibile trovare lo swagger per questa API in **Amministrazione > Accesso API** e fare clic sul collegamento "Documentazione API". Selezionare il tipo di API "Raccolta dati". Sotto l'intestazione *data_collection.data_collector*, seleziona l'API POST */collector/datasources* per questo esempio.



Se si imposta l'opzione *preEncrypted* su *True*, qualsiasi password passata tramite il comando API verrà trattata come **già crittografata**; l'API non crittograferà nuovamente la/le password. Quando crei la tua API, incolla semplicemente la password precedentemente crittografata nella posizione appropriata.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

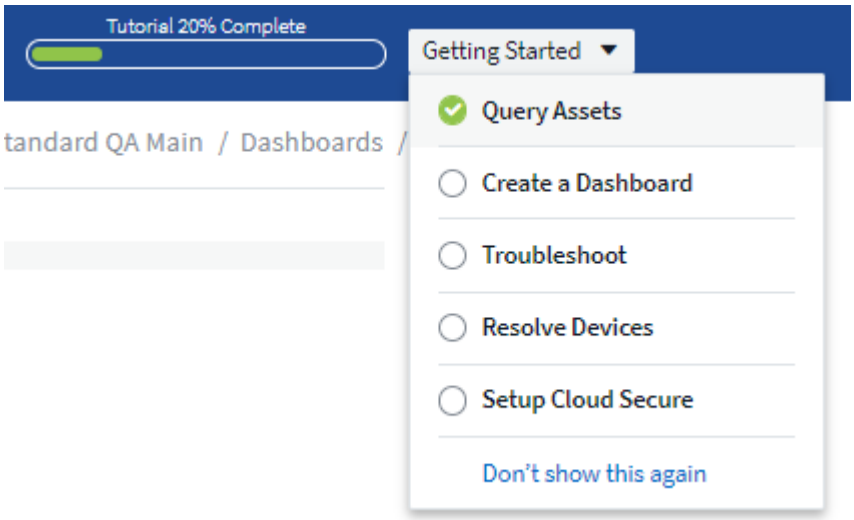
Iniziare

Introduzione ai tutorial video

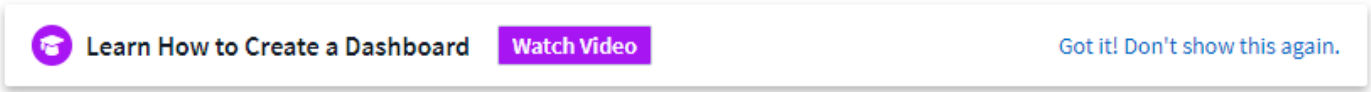
Apprendi in modo efficiente Data Infrastructure Insights con i nostri tutorial sulle funzionalità, dotati di guide video dettagliate e di una checklist di controllo dei progressi. Acquisisci competenze essenziali come la creazione di dashboard, la creazione di query, l'impostazione del monitoraggio e la risoluzione dei problemi tramite tutorial pratici pensati per renderti produttivo in tempi rapidi.

Lista di controllo e tutorial video

L'**elenco di controllo di avvio** visualizzato nel tenant di Data Infrastructure Insights contiene un elenco di diverse attività e concetti utili. Selezionando un elemento nella checklist si accede alla pagina Data Infrastructure Insights appropriata per quel concetto. Ad esempio, cliccando sulla voce *Crea una dashboard* si apre la pagina **Dashboard** Data Infrastructure Insights .



Nella parte superiore della pagina è presente un collegamento a un tutorial video che mostra come creare una dashboard. Puoi guardare il video tutte le volte che vuoi finché non clicchi su _Ho capito! Non mostrare più questo link per quel video. Il video è disponibile ogni volta che accedi alla pagina Dashboard, finché non lo chiudi.



Dopo aver guardato il video almeno una volta, la voce *Crea una dashboard* nella checklist risulta selezionata, a indicare che hai completato il tutorial. Puoi quindi procedere al tutorial successivo.

Puoi visualizzare i tutorial nell'ordine che preferisci, tutte le volte che vuoi, finché non li ignori.

Ignorare la checklist

L'elenco di controllo di avvio viene visualizzato finché non si fa clic sul collegamento *Non mostrare più* nella parte inferiore dell'elenco di controllo. Anche dopo aver eliminato la checklist, i tutorial restano disponibili in

ogni pagina appropriata Data Infrastructure Insights finché non li elimini tutti dalla barra dell'intestazione del messaggio.

Video tutorial

Guarda i seguenti video per saperne di più.

"Trasforma i dati grezzi in informazioni fruibili"

"Crea dashboard potenti con NetApp"

"Risoluzione dei problemi semplificata con VM Analyzer"

"Esplora e analizza con le query in Data Infrastructure Insights"

"Monitoraggio proattivo dell'infrastruttura con avvisi e monitor"

Raccolta dati

Come iniziare a raccogliere dati

Dopo esserti registrato a Data Infrastructure Insights e aver effettuato l'accesso al tuo ambiente per la prima volta, verrai guidato attraverso i seguenti passaggi per iniziare a raccogliere e gestire i dati.

I raccoglitori di dati scoprono informazioni dalle tue fonti di dati, come dispositivi di archiviazione, switch di rete e macchine virtuali. Le informazioni raccolte vengono utilizzate per l'analisi, la convalida, il monitoraggio e la risoluzione dei problemi.

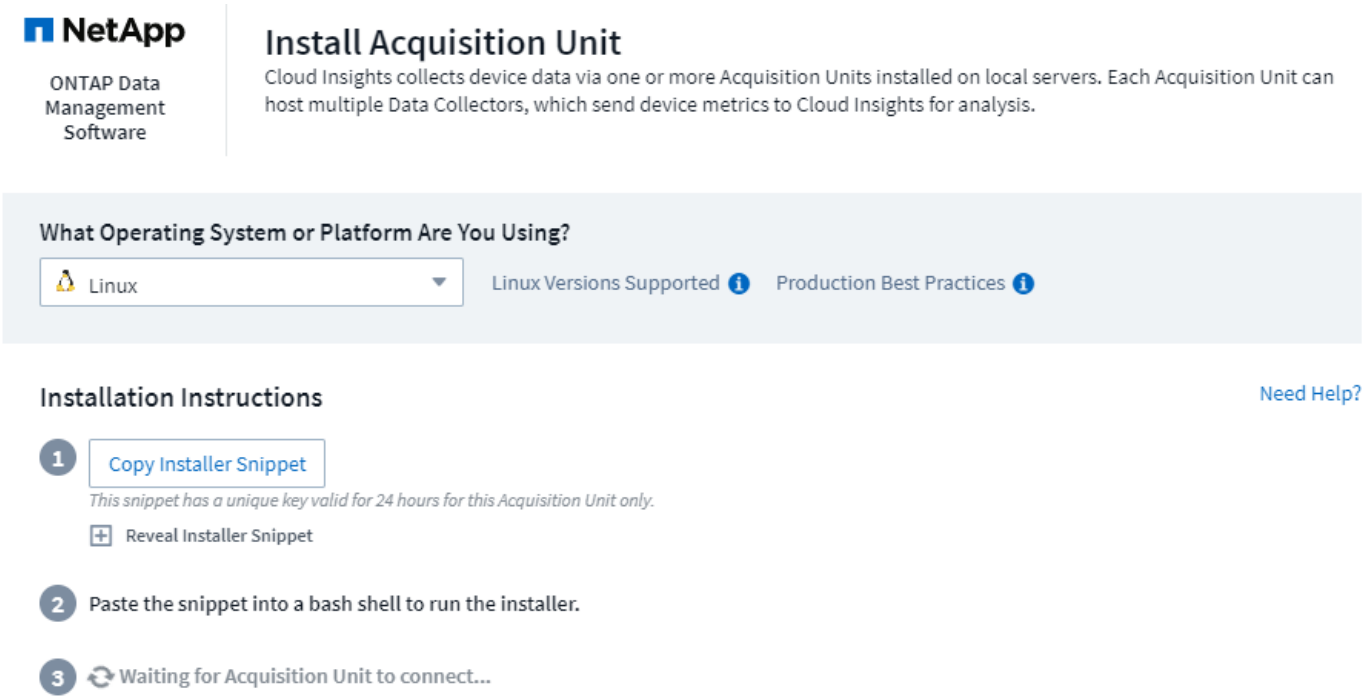
Data Infrastructure Insights dispone di tre tipi di collettori di dati:

- Infrastruttura (dispositivi di archiviazione, switch di rete, infrastruttura di elaborazione)
- Sistemi operativi (come VMware o Windows)
- Servizi (come Kafka)

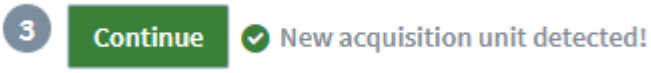
Seleziona il tuo primo raccoglitore dati tra i fornitori supportati e i modelli disponibili. In seguito sarà possibile aggiungere facilmente altri raccoglitori di dati.

Installare un'unità di acquisizione

Se hai selezionato un raccoglitore di dati *Infrastruttura*, è necessaria un'unità di acquisizione per immettere i dati in Data Infrastructure Insights. Sarà necessario scaricare e installare il software Acquisition Unit su un server o una macchina virtuale nel data center da cui si effettuerà la raccolta. Una singola unità di acquisizione può essere utilizzata per più raccoglitori di dati.



- Segui il"istruzioni" visualizzato per installare l'unità di acquisizione. Una volta installato il software Acquisition Unit, viene visualizzato il pulsante Continua ed è possibile procedere al passaggio successivo.



Se necessario, è possibile configurare ulteriori unità di acquisizione in un secondo momento. Ad esempio, potresti volere che diverse unità di acquisizione raccolgano informazioni dai data center in regioni diverse.

Configurare il Data Collector - Infrastruttura

Per i raccoglitori di dati *Infrastruttura*, ti verrà chiesto di compilare i campi del raccoglitore di dati presentati:

- Assegnare al raccoglitore dati un nome univoco e significativo.
- Immettere le credenziali (nome utente e password) per connettersi al dispositivo, se necessario.
- Compilare tutti gli altri campi obbligatori nelle sezioni *Configurazione* e *Configurazione avanzata*.
- Fare clic su **Aggiungi raccoglitore** per salvare il raccoglitore dati.

Sarà possibile configurare ulteriori raccoglitori di dati in un secondo momento.

Configurare il Data Collector - Sistemi operativi e servizi

Sistema operativo:

Per i raccoglitori di dati del *Sistema operativo*, scegliere una piattaforma (Linux, Windows) su cui installare un agente Data Infrastructure Insights . È necessario disporre di almeno un agente per raccogliere i dati dai Servizi. L'agente raccoglie anche dati dall'host stesso, per utilizzarli in Data Infrastructure Insights. Questi dati sono classificati come dati "Nodo" nei widget, ecc.

- Aprire un terminale o una finestra di comando sull'host dell'agente o sulla macchina virtuale e incollare il comando visualizzato per installare l'agente.

- Al termine dell'installazione, fare clic su **Completa installazione**.

Servizi:

Per i raccoglitori di dati *Servizio*, fare clic su un riquadro per aprire la pagina delle istruzioni per quel servizio.

- Scegli una piattaforma e una chiave di accesso agente.
- Se non hai un agente installato sulla piattaforma, segui le istruzioni per installarlo.
- Fare clic su **Continua** per aprire la pagina delle istruzioni del raccoglitore dati.
- Seguire le istruzioni per configurare il raccoglitore dati.
- Una volta completata la configurazione, fare clic su **Completa installazione**.

Aggiungi dashboard

A seconda del tipo di raccoglitore dati iniziale selezionato per la configurazione (archiviazione, switch, ecc.), verranno importate una o più dashboard pertinenti. Ad esempio, se hai configurato un raccoglitore di dati di archiviazione, verrà importato un set di dashboard relative all'archiviazione e una verrà impostata come home page di Data Infrastructure Insights . È possibile modificare la home page dall'elenco **Dashboard > Mostra tutte le dashboard**.

È possibile importare dashboard aggiuntive in un secondo momento oppure"crea il tuo" .

Questo è tutto ciò che c'è da fare

Dopo aver completato il processo di configurazione iniziale, l'ambiente inizierà a raccogliere dati.

Se il processo di configurazione iniziale viene interrotto (ad esempio, se si chiude la finestra del browser), sarà necessario seguire manualmente i passaggi:

- Scegli un raccoglitore di dati
- Installare un agente o un'unità di acquisizione se richiesto
- Configurare il Data Collector

Definizioni utili

Le seguenti definizioni possono essere utili quando si parla di collettori di dati o funzionalità Data Infrastructure Insights :

- Ciclo di vita del collezionista: un collezionista apparterrà a uno dei seguenti stati nel suo ciclo di vita:
  - **Anteprima**: Disponibile in quantità limitata o per un pubblico limitato. "Funzionalità di anteprima" e si prevede che i collettori di dati diventino GA dopo il periodo di anteprima. I periodi di anteprima variano in base al pubblico o alla funzionalità.
  - **GA**: una funzionalità o un raccoglitore di dati generalmente disponibile per tutti i clienti, in base all'edizione o al set di funzionalità.
  - **Obsoleto**: si applica ai raccoglitori di dati che non sono più funzionalmente sostenibili o che si prevede che non lo saranno più. I collettori di dati obsoleti vengono spesso sostituiti con collettori di dati più nuovi e funzionalmente aggiornati.
  - **Eliminato**: un raccoglitore di dati che è stato rimosso e non è più disponibile.
- Unità di acquisizione: un computer dedicato all'hosting di raccoglitori di dati, in genere una macchina virtuale. In genere questo computer si trova nello stesso data center/VPC degli elementi monitorati.

- Origine dati: un modulo per comunicare con uno stack hardware o software. Consiste in una configurazione e in un codice che vengono eseguiti sul computer AU per comunicare con il dispositivo.

Requisiti dell'unità di acquisizione

È necessario installare un'unità di acquisizione (AU) per acquisire informazioni dai collettori di dati dell'infrastruttura (archiviazione, VM, porta, EC2, ecc.). Prima di installare l'unità di acquisizione, è necessario assicurarsi che il tenant soddisfi i requisiti relativi a sistema operativo, CPU, memoria e spazio su disco.

Requisiti

Componente	Requisiti Linux	Requisiti di Windows
Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti: * AlmaLinux 9.5, 10 * Centos (64-bit): Stream 9 * Debian (64-bit): da 11 a 13 * OpenSUSE Leap 15.2 a 15.6, 16 * Oracle Enterprise Linux (64-bit): 8.10, 9.2, 9.4, 9.6, 10 * Red Hat (64-bit): 8.10, 9.2, 9.4, 9.6, 10 * Rocky 9.2 a 9.6 * SUSE Linux Enterprise Server 15 SP4 a 15 SP7, 16 * Ubuntu Server: 20.04, 22.04, 24.04 LTS * SELinux sulle piattaforme sopra indicate Questo computer non deve eseguire altri software a livello di applicazione. Si consiglia un server dedicato. Se si utilizza SELinux, si consiglia di eseguire i seguenti comandi sul sistema dell'unità di acquisizione: sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(/.*)?" sudo restorecon -R /opt/netapp/cloudinsights	Un computer che esegue una versione con licenza di uno dei seguenti: * Microsoft Windows 11 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows Server 2025 Su questo computer non deve essere in esecuzione nessun altro software a livello di applicazione. Si consiglia un server dedicato.
processore	2 core della CPU	Stesso
Memoria	8 GB di RAM	Stesso
Spazio disponibile su disco	50 GB (100 GB consigliati) Per Linux, lo spazio su disco dovrebbe essere allocato in questo modo: /opt/netapp 10 GB (20 GB per ambienti di grandi dimensioni) /var/log/netapp 40 GB (80 GB per ambienti di grandi dimensioni) /tmp almeno 1 GB disponibile durante l'installazione	50 GB

Rete	Sono richiesti una connessione Ethernet da 100 Mbps/1 Gbps, un indirizzo IP statico e una connettività sulla porta 80 o 443 (in uscita) dall'unità di acquisizione a *.cloudinsights.netapp.com o al tenant di Data Infrastructure Insights (ad esempio https://<tenant_id>.c01.cloudinsights.netapp.com). Per i requisiti tra l'unità di acquisizione e ciascun raccoglitore di dati, fare riferimento alle istruzioni per l'"Responsabile della raccolta dati" . Se la tua organizzazione richiede l'utilizzo di un proxy per l'accesso a Internet, potrebbe essere necessario comprendere il comportamento del proxy della tua organizzazione e cercare determinate eccezioni affinché Data Infrastructure Insights funzioni. Ad esempio, la tua organizzazione blocca l'accesso per impostazione predefinita e consente l'accesso solo a specifici siti web/domini in via eccezionale? In tal caso, sarà necessario aggiungere il seguente dominio all'elenco delle eccezioni: *.cloudinsights.netapp.com Per ulteriori informazioni, leggere la sezione Proxy"qui (Linux)" O"qui (Windows)" .	Stesso
Permessi	Autorizzazioni Sudo sul server Acquisition Unit. /tmp deve essere montato con funzionalità exec.	Autorizzazioni di amministratore sul server Acquisition Unit
Scansione antivirus		Durante l'installazione è necessario disattivare completamente tutti gli scanner antivirus. Dopo l'installazione, i percorsi utilizzati dal software Acquisition Unit devono essere esclusi dalla scansione antivirus.

Ulteriori raccomandazioni

- Per un audit e una rendicontazione dei dati accurati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'unità di acquisizione utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

Per quanto riguarda le dimensioni

È possibile iniziare con una Data Infrastructure Insights Acquisition Unit con soli 8 GB di memoria e 50 GB di spazio su disco; tuttavia, per ambienti più grandi, è opportuno porsi le seguenti domande:

Ti aspetti di:

- Scopri più di 2500 macchine virtuali o 10 grandi cluster ONTAP (> 2 nodi), array Symmetrix o HDS/HPE VSP/XP su questa unità di acquisizione?
- Distribuire 75 o più raccoglitori di dati totali su questa unità di acquisizione?

Per ogni risposta "Sì" sopra, si consiglia di aggiungere 8 GB di memoria e 50 GB di spazio su disco all'AU. Ad esempio, se hai risposto "Sì" a entrambe le domande, dovresti implementare un sistema con 24 GB di memoria e 150 GB o più di spazio su disco. Su Linux, lo spazio su disco da aggiungere alla posizione del registro.

Per ulteriori domande sul dimensionamento, contattare l'assistenza NetApp .

Configurazione delle unità di acquisizione

Data Infrastructure Insights raccoglie i dati dei dispositivi utilizzando una o più unità di acquisizione installate su server locali. Ogni unità di acquisizione può ospitare più Data Collector, che inviano le metriche dei dispositivi a Data Infrastructure Insights per l'analisi.

In questo argomento viene descritto come aggiungere unità di acquisizione e vengono descritti i passaggi aggiuntivi richiesti quando l'ambiente utilizza un proxy.

Per un audit e una rendicontazione dei dati accurati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'unità di acquisizione utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

Scopri di più sulla sicurezza Data Infrastructure Insights"Qui" .

Aggiunta di un'unità di acquisizione Linux

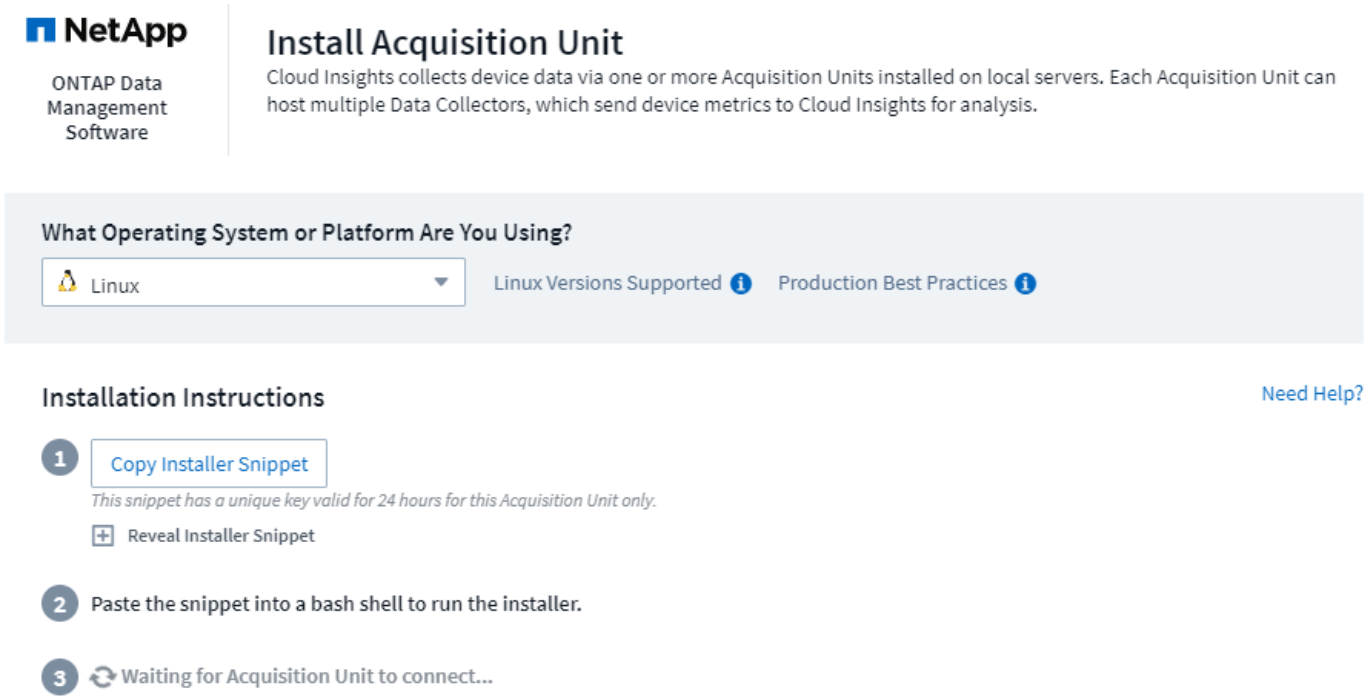
Prima di iniziare

- Se il sistema utilizza un proxy, è necessario impostare le variabili di ambiente del proxy prima di installare l'unità di acquisizione. Per ulteriori informazioni, consultare Impostazione delle variabili di ambiente proxy .

Passaggi per l'installazione dell'unità di acquisizione Linux

1. Accedi come amministratore o proprietario dell'account al tuo ambiente Data Infrastructure Insights .
2. Fare clic su **Osservabilità > Collezionisti > Unità di acquisizione > +Unità di acquisizione**

   Il sistema visualizza la finestra di dialogo *Installa unità di acquisizione*. Scegli Linux.



1. Verificare che il server o la VM che ospita l'unità di acquisizione soddisfi i requisiti di sistema consigliati.
2. Verificare che sul server sia installata una versione supportata di Linux. Fare clic su *Versioni del sistema operativo supportate (i)* per un elenco delle versioni supportate.
3. Copiare il frammento di comando Installazione nella finestra di dialogo in una finestra del terminale sul server o sulla macchina virtuale che ospiterà l'unità di acquisizione.
4. Incolla ed esegui il comando nella shell Bash.

Dopo aver finito

- Fare clic su **Osservabilità > Collettori > Unità di acquisizione** per verificare lo stato delle Unità di acquisizione.
- È possibile accedere ai registri dell'unità di acquisizione in /var/log/netapp/cloudinsights/acq/acq.log
- Utilizzare il seguente script per controllare l'unità di acquisizione:
  - cloudinsights-service.sh (arresta, avvia, riavvia, controlla lo stato)
- Utilizzare il seguente script per disinstallare l'unità di acquisizione:
  - cloudinsights-uninstall.sh

Impostazione delle variabili di ambiente proxy

Per gli ambienti che utilizzano un proxy, è necessario impostare le variabili di ambiente del proxy prima di aggiungere l'unità di acquisizione. Le istruzioni per la configurazione del proxy sono fornite nella finestra di dialogo *Aggiungi unità di acquisizione*.

1. Fai clic su + in *Hai un server proxy?*
2. Copia i comandi in un editor di testo e imposta le variabili proxy secondo necessità.

   Nota: tieni presente le restrizioni sui caratteri speciali nei campi nome utente e password del proxy: nel campo nome utente sono consentiti '%' e '!'. Nel campo password sono consentiti i caratteri ':', '%' e '!'.

3. Eseguire il comando modificato in un terminale utilizzando la shell Bash.
4. Installare il software Acquisition Unit.

Configurazione proxy

L'unità di acquisizione utilizza l'autenticazione reciproca/bidirezionale per connettersi al server Data Infrastructure Insights . Per l'autenticazione, il certificato client deve essere trasmesso al server Data Infrastructure Insights . Per raggiungere questo obiettivo, il proxy deve essere configurato per inoltrare la richiesta https al server Data Infrastructure Insights senza decrittografare i dati.

Il modo più semplice per farlo è specificare la configurazione jolly nel proxy/firewall per comunicare con Data Infrastructure Insights, ad esempio:

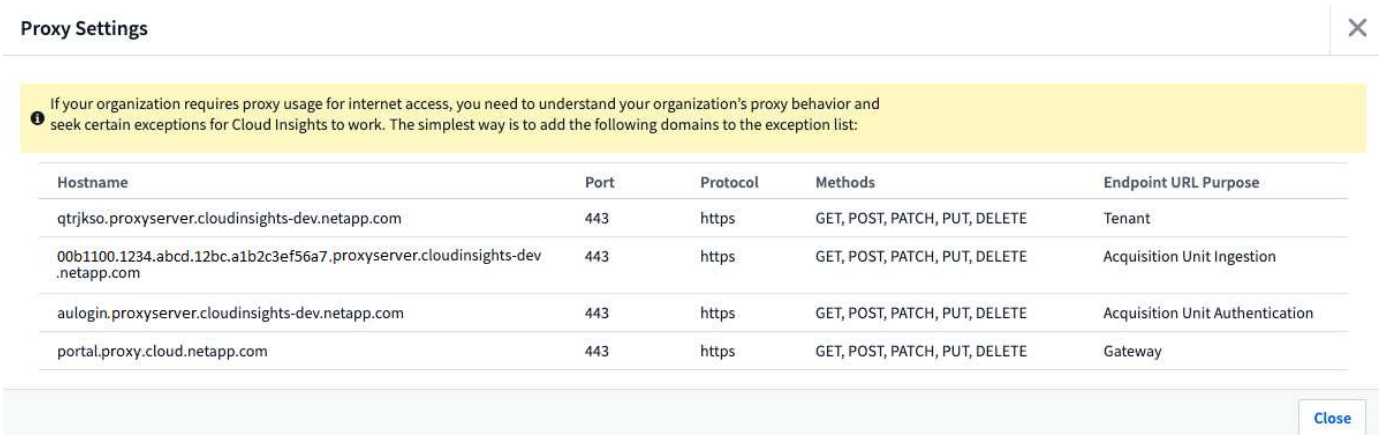
```
*.cloudinsights.netapp.com
```

> L'uso di un asterisco (*) come carattere jolly è comune, ma la configurazione del proxy/firewall potrebbe utilizzare un formato diverso. Consultare la documentazione del proxy per garantire la corretta specifica dei caratteri jolly nel proprio ambiente.

Ulteriori informazioni sulla configurazione del proxy sono disponibili in NetApp"Base di conoscenza" .

Visualizzazione degli URL proxy

Puoi visualizzare gli URL degli endpoint proxy facendo clic sul collegamento **Impostazioni proxy** quando scegli un raccoglitore dati durante l'onboarding oppure sul collegamento in *Impostazioni proxy* nella pagina **Guida > Supporto**. Viene visualizzata una tabella come la seguente.



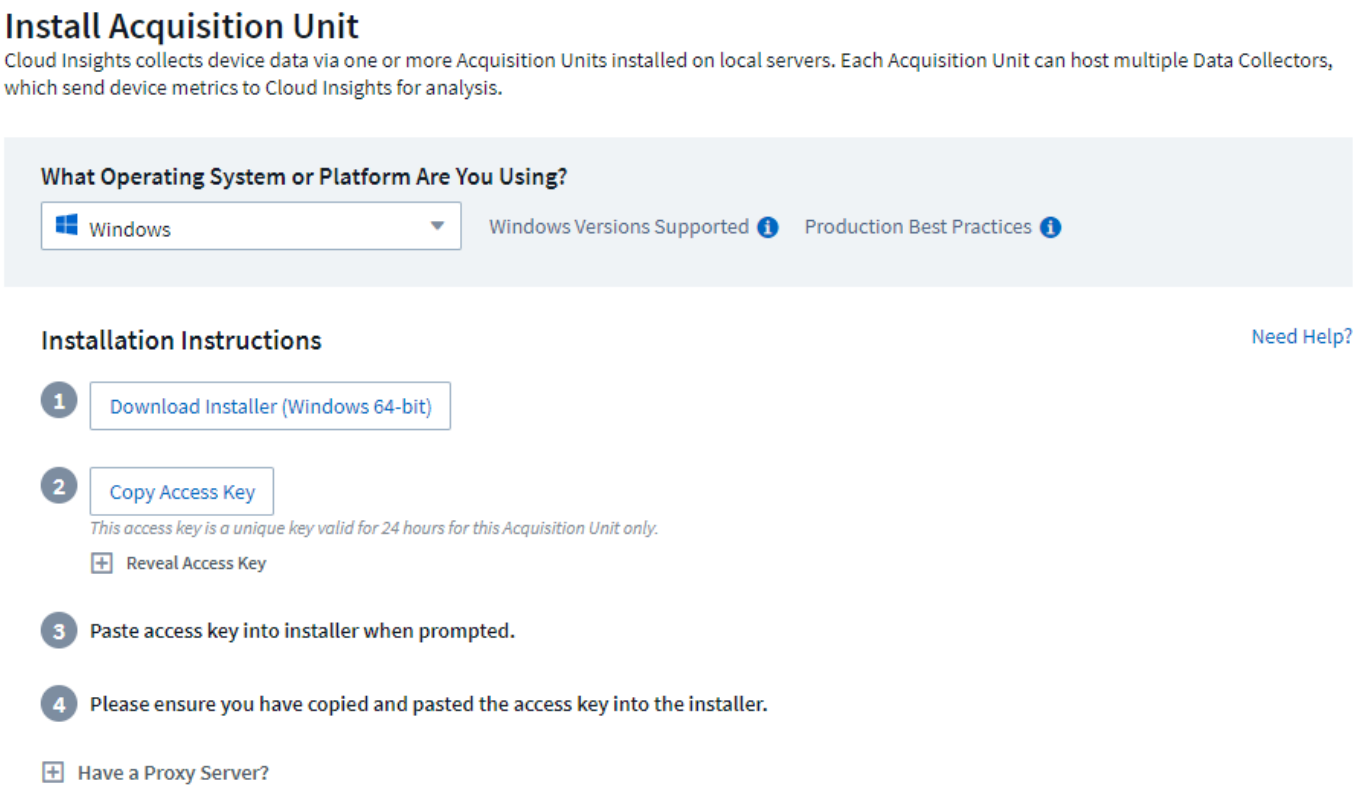
Se sul tenant è presente Workload Security, in questo elenco verranno visualizzati anche gli URL degli endpoint configurati.

Aggiunta di un'unità di acquisizione Windows

Passaggi per l'installazione dell'unità di acquisizione Windows

1. Accedere al server/VM dell'unità di acquisizione come utente con autorizzazioni di amministratore.
2. Su quel server, apri una finestra del browser e accedi al tuo ambiente Data Infrastructure Insights come amministratore o proprietario dell'account.
3. Fare clic su **Osservabilità > Collettori > Unità di acquisizione > +Unità di acquisizione**.

Il sistema visualizza la finestra di dialogo *Installa unità di acquisizione*. Scegli Windows.



1. Verificare che il server o la VM che ospita l'unità di acquisizione soddisfi i requisiti di sistema consigliati.
2. Verificare che sul server sia installata una versione supportata di Windows. Fare clic su *Versioni del sistema operativo supportate (i)* per un elenco delle versioni supportate.
3. Fare clic sul pulsante **Scarica programma di installazione (Windows a 64 bit)**.
4. Copia la chiave di accesso. Ne avrai bisogno durante l'installazione.
5. Sul server/VM dell'unità di acquisizione, eseguire il programma di installazione scaricato.
6. Quando richiesto, incollare la chiave di accesso nella procedura guidata di installazione.
7. Durante l'installazione, ti verrà offerta l'opportunità di fornire le impostazioni del tuo server proxy.

Dopo aver finito

- Fare clic su * > Osservabilità > Collettori > Unità di acquisizione* per verificare lo stato delle Unità di acquisizione.
- È possibile accedere al registro dell'unità di acquisizione in <directory di installazione>\ Cloud Insights\Acquisition Unit\log\acq.log
- Utilizzare lo script seguente per arrestare, avviare, riavviare o controllare lo stato dell'unità di acquisizione:

```
cloudinsights-service.sh
```

Configurazione proxy

L'unità di acquisizione utilizza l'autenticazione reciproca/bidirezionale per connettersi al server Data

Infrastructure Insights . Per l'autenticazione, il certificato client deve essere trasmesso al server Data Infrastructure Insights . Per raggiungere questo obiettivo, il proxy deve essere configurato per inoltrare la richiesta https al server Data Infrastructure Insights senza decrittografare i dati.

Il modo più semplice per farlo è specificare la configurazione jolly nel proxy/firewall per comunicare con Data Infrastructure Insights, ad esempio:

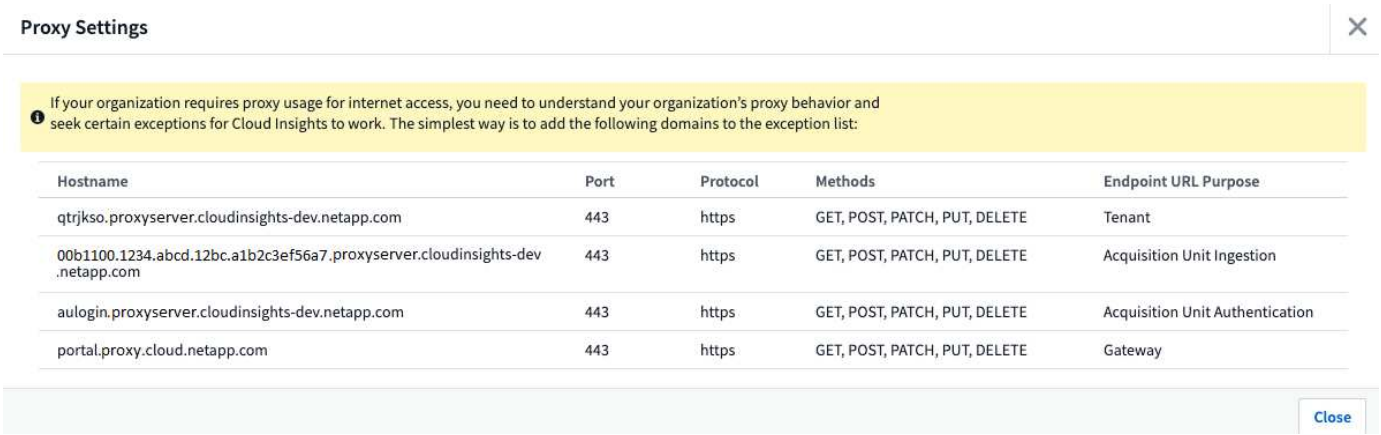
```
*.cloudinsights.netapp.com
```

L'uso di un asterisco (*) come carattere jolly è comune, ma la configurazione del proxy/firewall potrebbe utilizzare un formato diverso. Consultare la documentazione del proxy per garantire la corretta specifica dei caratteri jolly nel proprio ambiente.

Ulteriori informazioni sulla configurazione del proxy sono disponibili in NetApp"Base di conoscenza" .

Visualizzazione degli URL proxy

Puoi visualizzare gli URL degli endpoint proxy facendo clic sul collegamento **Impostazioni proxy** quando scegli un raccoglitore dati durante l'onboarding oppure sul collegamento in *Impostazioni proxy* nella pagina **Guida > Supporto**. Viene visualizzata una tabella come la seguente.



Se sul tenant è presente Workload Security, in questo elenco verranno visualizzati anche gli URL degli endpoint configurati.

Disinstallazione di un'unità di acquisizione

Per disinstallare il software Acquisition Unit, procedere come segue:

Finestre:

Se si sta disinstallando un'unità di acquisizione **Windows**:

1. Sul server/VM dell'unità di acquisizione, aprire il Pannello di controllo e selezionare **Disinstalla un programma**. Selezionare il programma Data Infrastructure Insights Acquisition Unit per la rimozione.
2. Fare clic su Disinstalla e seguire le istruzioni.

Linux:

Se si sta disinstallando un'unità di acquisizione **Linux**:

1. Sul server/VM dell'unità di acquisizione, eseguire il seguente comando:

```
 sudo cloudinsights-uninstall.sh -p
. Per assistenza con la disinstallazione, eseguire:
```

```
sudo cloudinsights-uninstall.sh --help
```

Windows e Linux:

Dopo aver disinstallato l'AU:

1. In Data Infrastructure Insights, vai su **Osservabilità > Collettori e seleziona la scheda *Unità di acquisizione**.
2. Fare clic sul pulsante Opzioni a destra dell'unità di acquisizione che si desidera disinstallare e selezionare *Elimina*. È possibile eliminare un'unità di acquisizione solo se non le sono assegnati collettori di dati.

> Non è possibile eliminare un'unità di acquisizione (AU) a cui sono collegati dei collettori dati. Spostare tutti i raccoglitori di dati dell'AU in un'altra AU (modificare il raccoglitore e selezionare semplicemente un'AU diversa) prima di eliminare l'AU originale.

Per la risoluzione del dispositivo viene utilizzata un'unità di acquisizione contrassegnata da una stella. Prima di rimuovere questa AU, è necessario selezionarne un'altra da utilizzare per la risoluzione del dispositivo. Passa il mouse su un'AU diversa e apri il menu "tre puntini" per selezionare "Usa per risoluzione dispositivo".

Reinstallazione di un'unità di acquisizione

Per reinstallare un'unità di acquisizione sullo stesso server/VM, è necessario seguire questi passaggi:

Prima di iniziare

Prima di reinstallare un'unità di acquisizione, è necessario configurare un'unità di acquisizione temporanea su un server/VM separato.

Passi

1. Accedere al server/VM dell'unità di acquisizione e disinstallare il software AU.
2. Accedi al tuo ambiente Data Infrastructure Insights e vai su **Osservabilità > Collettori**.
3. Per ogni raccoglitore di dati, fare clic sul menu Opzioni a destra e selezionare *Modifica*. Assegnare il raccoglitore dati all'unità di acquisizione temporanea e fare clic su **Salva**.

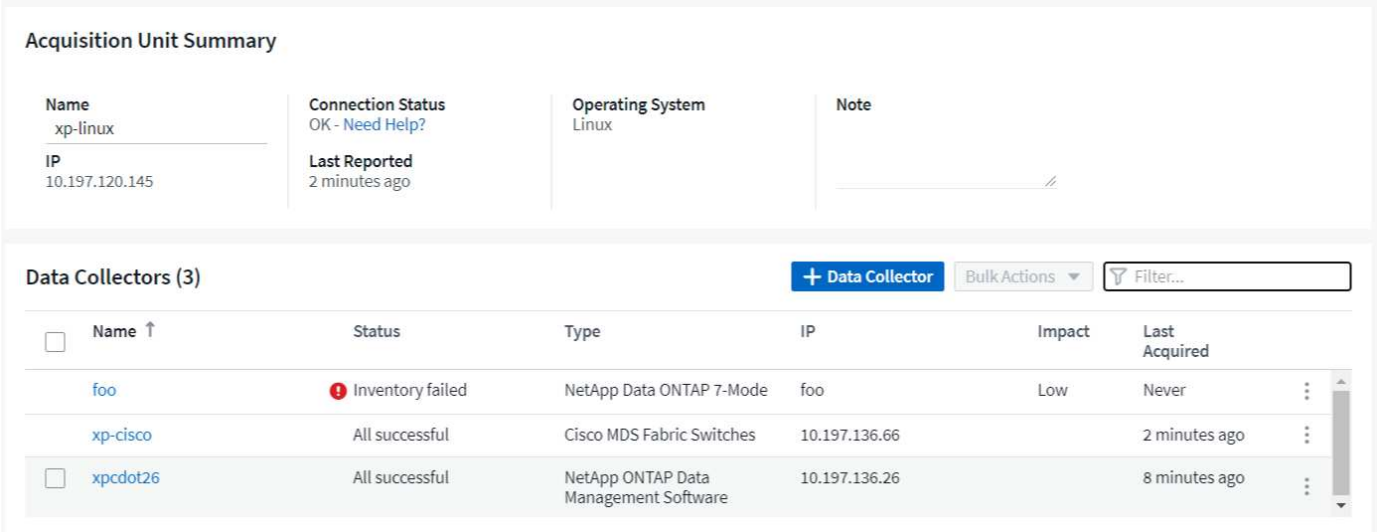
È anche possibile selezionare più raccoglitori di dati dello stesso tipo e fare clic sul pulsante **Azioni in blocco**. Selezionare *Modifica* e assegnare i raccoglitori di dati all'Unità di acquisizione temporanea.

4. Dopo aver spostato tutti i collettori di dati nell'unità di acquisizione temporanea, andare su **Osservabilità > Collettori** e selezionare la scheda **Unità di acquisizione**.
5. Fare clic sul pulsante Opzioni a destra dell'unità di acquisizione che si desidera reinstallare e selezionare *Elimina*. È possibile eliminare un'unità di acquisizione solo se non le sono assegnati collettori di dati.
6. Ora puoi reinstallare il software Acquisition Unit sul server/VM originale. Fare clic su **+Unità di acquisizione** e seguire le istruzioni sopra riportate per installare l'Unità di acquisizione.
7. Una volta reinstallata l'Unità di acquisizione, riassegnare i raccoglitori di dati all'Unità di acquisizione.

Visualizzazione dei dettagli AU

La pagina dei dettagli dell'Unità di acquisizione (AU) fornisce informazioni utili su un'AU, nonché informazioni utili per la risoluzione dei problemi. La pagina dei dettagli dell'AU contiene le seguenti sezioni:

- Una sezione **riepilogo** che mostra quanto segue:
  - **Nome** e **IP** dell'Unità di acquisizione
  - Stato attuale della connessione dell'AU
  - **Ultimo report** tempo di polling del raccoglitore dati riuscito
  - Il **Sistema operativo** della macchina AU
  - Qualche **Nota** attuale per l'UA. Utilizzare questo campo per inserire un commento per l'AU. Il campo visualizza la nota aggiunta più di recente.
- Una tabella dei **raccoglitori di dati** dell'AU che mostra, per ciascun raccoglitore di dati:
  - **Nome** - Fai clic su questo collegamento per accedere alla pagina dei dettagli del raccoglitore dati con informazioni aggiuntive
  - **Stato** - Informazioni su successo o errore
  - **Tipo** - Fornitore/modello
  - Indirizzo **IP** del raccoglitore dei dati
  - Livello attuale di **impatto**
  - **Ultima acquisizione** - data dell'ultimo polling riuscito del raccoglitore dati



Per ogni raccoglitore di dati, puoi cliccare sul menu "tre puntini" per clonare, modificare, interrogare o eliminare il raccoglitore di dati. È anche possibile selezionare più raccoglitori di dati in questo elenco per eseguire su di essi azioni in blocco.

Per riavviare l'Unità di acquisizione, fare clic sul pulsante **Riavvia** nella parte superiore della pagina. Fai clic su questo pulsante per tentare di **Ripristinare la connessione** all'AU in caso di problemi di connessione.

Configurazione di un agente per la raccolta di dati (Windows/Linux)

Gli utilizzi di Data Infrastructure Insights"Telegrafo" come suo agente per la raccolta dei dati di integrazione. Telegraf è un agente server basato su plugin che può essere utilizzato per raccogliere e segnalare metriche, eventi e registri. I plugin di input vengono utilizzati per raccogliere le informazioni desiderate nell'agente accedendo direttamente al sistema/sistema operativo, chiamando API di terze parti o ascoltando flussi configurati (ad esempio Kafka, statsD, ecc.). I plugin di output vengono utilizzati per inviare le metriche, gli eventi e i log raccolti dall'agente a Data Infrastructure Insights.

Per informazioni sull'installazione su Kubernetes, vedere"Operatore di monitoraggio NetApp Kubernetes" pagina.

Per un audit e una segnalazione dei dati accurati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'agente utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

Se si desidera verificare i file di installazione prima di installare l'agente, vedere la sezione seguente suVerifica dei checksum del pacchetto Telegraf .

Installazione di un agente

Se si sta installando un Service Data Collector e non è ancora stato configurato un Agent, verrà richiesto di installare prima un Agent per il sistema operativo appropriato. In questo argomento vengono fornite istruzioni per l'installazione dell'agente Telegraf sui seguenti sistemi operativi:

- Finestre
- RHEL e CentOS
- Ubuntu e Debian

Per installare un agente, indipendentemente dalla piattaforma utilizzata, è necessario innanzitutto effettuare le seguenti operazioni:

1. Accedi all'host che utilizzerai per il tuo agente.
2. Accedi al tuo ambiente Data Infrastructure Insights e vai su **Osservabilità > Collettori**.
3. Fare clic su **+Data Collector** e scegliere un data collector da installare.
4. Scegli la piattaforma appropriata per il tuo host (Windows, Linux)
5. Seguire i passaggi rimanenti per ciascuna piattaforma.

Una volta installato un agente su un host, non è necessario installarlo nuovamente sullo stesso host.

Dopo aver installato un agente su un server/VM, Data Infrastructure Insights raccoglie le metriche da quel sistema, oltre a raccoglierle da tutti i collettori dati configurati. Queste metriche vengono raccolte come"Metriche "Nodo"" .

Se si utilizza un proxy, leggere le istruzioni del proxy per la propria piattaforma prima di installare l'agente Telegraf.

Posizioni dei registri

Per impostazione predefinita, i messaggi di registro di Telegraf vengono reindirizzati da stdout ai seguenti file di registro:

- RHEL/CentOS: /var/log/telegraf/telegraf.log
- Ubuntu/Debian: /var/log/telegraf/telegraf.log
- Windows: C:\Programmi\telegraf\telegraf.log

Finestre

Prerequisiti:

- PowerShell deve essere installato
- Se si utilizza un proxy, è necessario seguire le istruzioni nella sezione **Configurazione del supporto proxy per Windows**.

Configurazione del supporto proxy per Windows

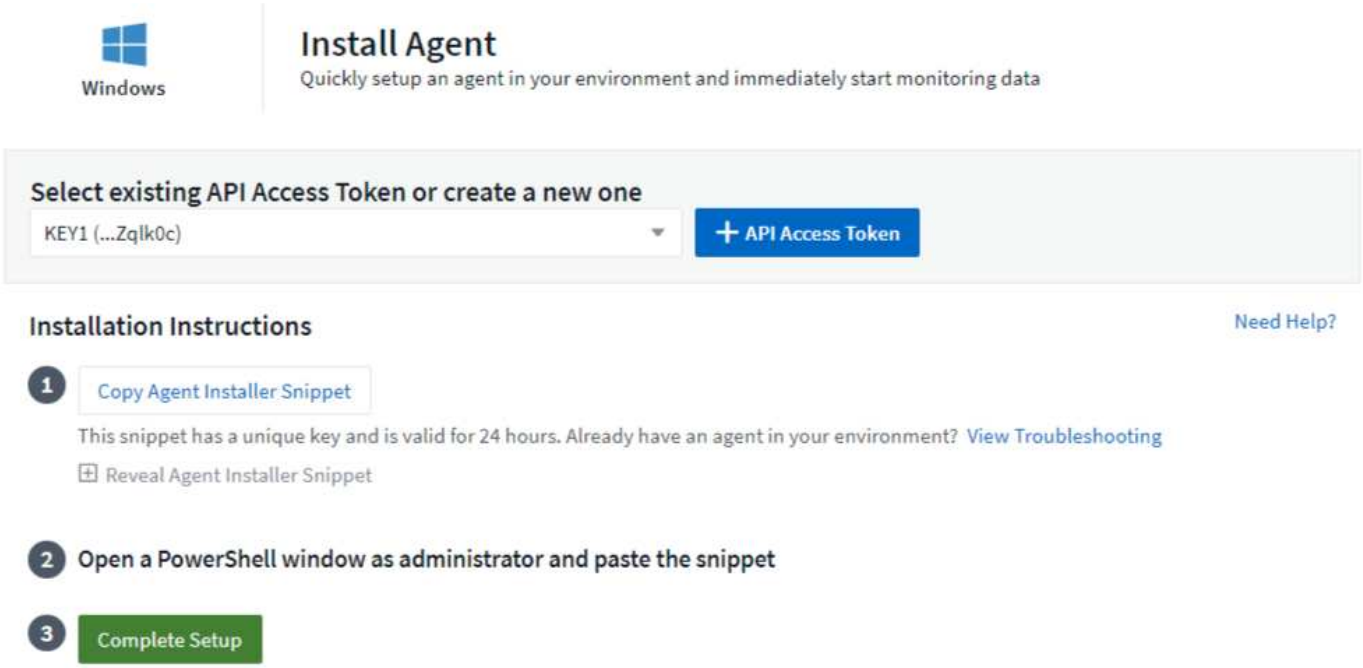
Se il tuo ambiente utilizza un proxy, leggi questa sezione prima di procedere all'installazione.

I passaggi seguenti descrivono le azioni necessarie per impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, gli utenti potrebbero dover impostare anche la variabile di ambiente *no_proxy*.

Per i sistemi che risiedono dietro un proxy, procedere come segue per impostare le variabili di ambiente *https_proxy* e/o *http_proxy* **PRIMA** di installare l'agente Telegraf:

```
[System.Environment]:SetEnvironmentVariable("https_proxy",
"<proxy_server>:<proxy_port>", [System.EnvironmentVariableTarget]:Machine)
```

Installazione dell'agente



Passaggi per installare l'agente su Windows:

1. Scegli una chiave di accesso agente.
2. Copiare il blocco di comando dalla finestra di dialogo di installazione dell'agente. È possibile fare clic sull'icona degli appunti per copiare rapidamente il comando negli appunti.
3. Aprire una finestra di PowerShell
4. Incollare il comando nella finestra di PowerShell e premere Invio.
5. Il comando scaricherà il programma di installazione dell'agente appropriato, lo installerà e imposterà una configurazione predefinita. Al termine, il servizio agente verrà riavviato. Il comando ha una chiave univoca ed è valido per 24 ore.
6. Fare clic su **Fine** o **Continua**

Dopo aver installato l'agente, è possibile utilizzare i seguenti comandi per avviare/arrestare il servizio:

```
Start-Service telegraf
Stop-Service telegraf
```

Disinstallazione dell'agente

Per disinstallare l'agente su Windows, procedere come segue in una finestra di PowerShell:

1. Arrestare ed eliminare il servizio Telegraf:

   ```
   Stop-Service telegraf
   sc.exe delete telegraf
   ```

2. Rimuovere il certificato dal trustore:

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. Eliminare la cartella *C:\Programmi\telegraf* per rimuovere i file binari, di registro e di configurazione
4. Rimuovere la chiave *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* dal registro

Aggiornamento dell'agente

Per aggiornare l'agente Telegraf, procedere come segue:

1. Arrestare ed eliminare il servizio Telegraf:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Eliminare la chiave *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* dal registro
3. Elimina *C:\Programmi\telegraf\telegraf.conf*
4. Elimina *C:\Programmi\telegraf\telegraf.exe*
5. "Installa il nuovo agente" .

RHEL e CentOS

Prerequisiti:

- Devono essere disponibili i seguenti comandi: curl, sudo, ping, sha256sum, openssl e dmidecode
- Se si utilizza un proxy, è necessario seguire le istruzioni nella sezione **Configurazione del supporto proxy per RHEL/CentOS**.

Configurazione del supporto proxy per RHEL/CentOS

Se il tuo ambiente utilizza un proxy, leggi questa sezione prima di procedere all'installazione.

I passaggi seguenti descrivono le azioni necessarie per impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, gli utenti potrebbero dover impostare anche la variabile di ambiente *no_proxy*.

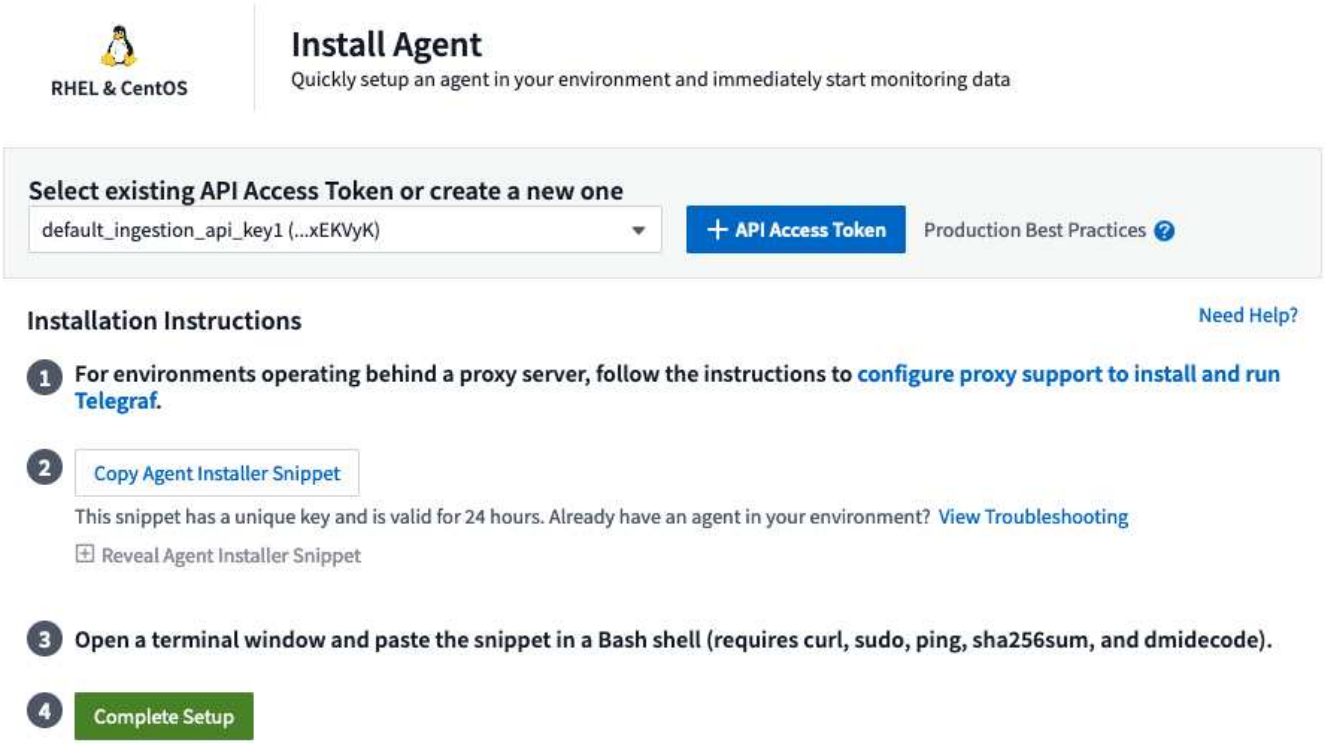
Per i sistemi che risiedono dietro un proxy, eseguire i seguenti passaggi **PRIMA** di installare l'agente Telegraf:

1. Imposta le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Crea _/etc/default/telegraf_ e inserisci le definizioni per le
variabili _https_proxy_ e/o _http_proxy_:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installazione dell'agente



Passaggi per installare l'agente su RHEL/CentOS:

1. Scegli una chiave di accesso agente.
2. Copiare il blocco di comando dalla finestra di dialogo di installazione dell'agente. È possibile fare clic sull'icona degli appunti per copiare rapidamente il comando negli appunti.
3. Aprire una finestra Bash
4. Incolla il comando nella finestra Bash e premi Invio.
5. Il comando scaricherà il programma di installazione dell'agente appropriato, lo installerà e imposterà una configurazione predefinita. Al termine, il servizio agente verrà riavviato. Il comando ha una chiave univoca ed è valido per 24 ore.
6. Fare clic su **Fine** o **Continua**

Dopo aver installato l'agente, è possibile utilizzare i seguenti comandi per avviare/arrestare il servizio:

Se il tuo sistema operativo utilizza systemd (CentOS 7+ e RHEL 7+):

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Se il tuo sistema operativo non utilizza systemd (CentOS 7+ e RHEL 7+):

```
sudo service telegraf start
sudo service telegraf stop
```

Disinstallazione dell'agente

Per disinstallare l'agente su RHEL/CentOS, in un terminale Bash, procedere come segue:

1. Interrompere il servizio Telegraf:

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Rimuovere l'agente Telegraf:

```
 yum remove telegraf
. Rimuovere eventuali file di configurazione o di registro rimasti:
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Aggiornamento dell'agente

Per aggiornare l'agente Telegraf, procedere come segue:

1. Interrompere il servizio telegrafico:

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Rimuovere il precedente agente telegrafico:

```
 yum remove telegraf
. xref:{relative_path}#rhel-and-centos["Installa il nuovo agente"] .
```

Ubuntu e Debian

Prerequisiti:

- Devono essere disponibili i seguenti comandi: curl, sudo, ping, sha256sum, openssl e dmidecode

- Se si utilizza un proxy, è necessario seguire le istruzioni nella sezione **Configurazione del supporto proxy per Ubuntu/Debian**.

Configurazione del supporto proxy per Ubuntu/Debian

Se il tuo ambiente utilizza un proxy, leggi questa sezione prima di procedere all'installazione.

I passaggi seguenti descrivono le azioni necessarie per impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, gli utenti potrebbero dover impostare anche la variabile di ambiente *no_proxy*.

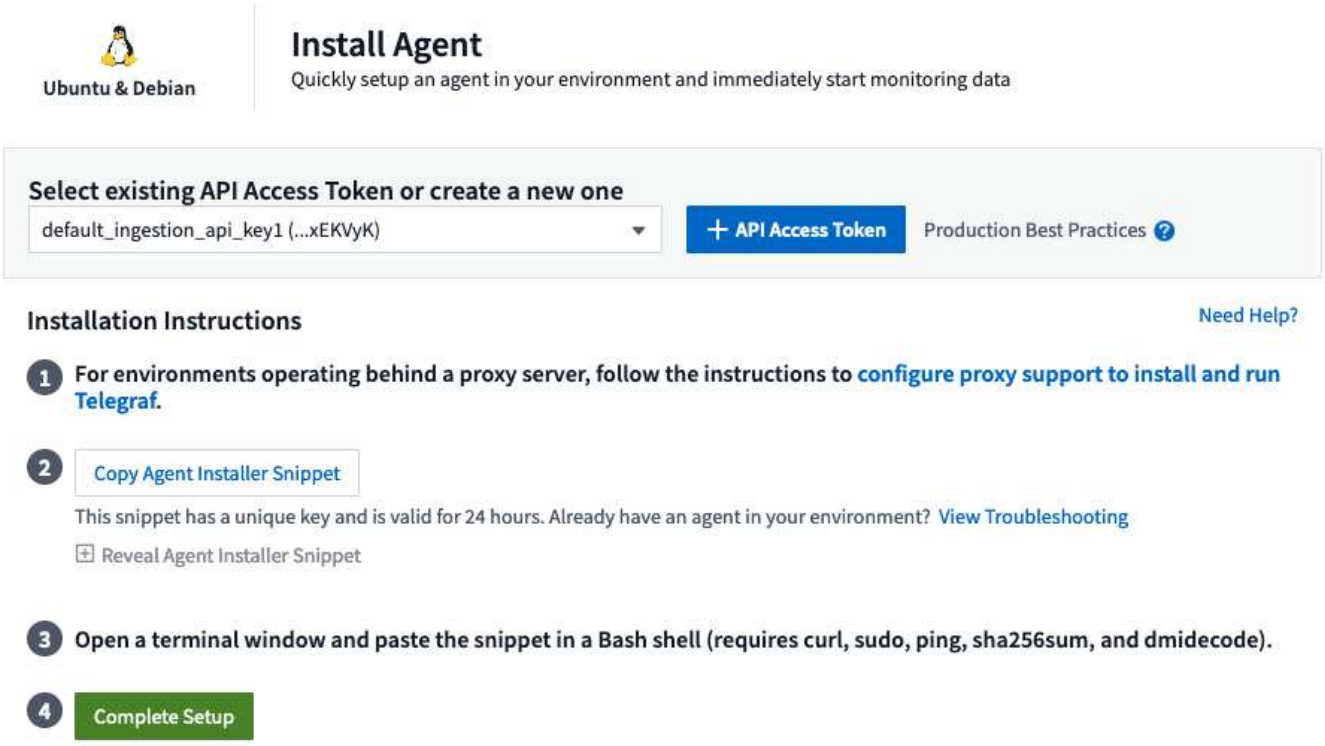
Per i sistemi che risiedono dietro un proxy, eseguire i seguenti passaggi **PRIMA** di installare l'agente Telegraf:

1. Imposta le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Crea /etc/default/telegraf e inserisci le definizioni per le variabili
_https_proxy_ e/o _http_proxy_:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installazione dell'agente



Passaggi per installare l'agente su Debian o Ubuntu:

1. Scegli una chiave di accesso agente.
2. Copiare il blocco di comando dalla finestra di dialogo di installazione dell'agente. È possibile fare clic sull'icona degli appunti per copiare rapidamente il comando negli appunti.
3. Aprire una finestra Bash
4. Incolla il comando nella finestra Bash e premi Invio.
5. Il comando scaricherà il programma di installazione dell'agente appropriato, lo installerà e imposterà una configurazione predefinita. Al termine, il servizio agente verrà riavviato. Il comando ha una chiave univoca ed è valido per 24 ore.
6. Fare clic su **Fine** o **Continua**

Dopo aver installato l'agente, è possibile utilizzare i seguenti comandi per avviare/arrestare il servizio:

Se il tuo sistema operativo utilizza systemd:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Se il tuo sistema operativo non utilizza systemd:

```
sudo service telegraf start
sudo service telegraf stop
```

Disinstallazione dell'agente

Per disinstallare l'agente su Ubuntu/Debian, in un terminale Bash, eseguire quanto segue:

1. Interrompere il servizio Telegraf:

   ```
   systemctl stop telegraf (If your operating system is using systemd)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Rimuovere l'agente Telegraf:

   ```
    dpkg -r telegraf
   . Rimuovere eventuali file di configurazione o di registro rimasti:
   ```

   ```
   rm -rf /etc/telegraf*
   rm -rf /var/log/telegraf*
   ```

Aggiornamento dell'agente

Per aggiornare l'agente Telegraf, procedere come segue:

1. Interrompere il servizio telegrafico:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Rimuovere il precedente agente telegrafico:

```
 dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["Installa il nuovo agente"] .
```

Verifica dei checksum del pacchetto Telegraf

Il programma di installazione dell'agente Data Infrastructure Insights esegue controlli di integrità, ma alcuni utenti potrebbero voler eseguire le proprie verifiche prima di installare il binario Telegraf scaricato. Ciò può essere fatto scaricando il programma di installazione e generando un checksum per il pacchetto scaricato, quindi confrontando il checksum con il valore mostrato nelle istruzioni di installazione.

Scarica il pacchetto di installazione senza installare

Per eseguire un'operazione di solo download (in contrapposizione al download e installazione predefinito), gli utenti possono modificare il comando di installazione dell'agente ottenuto dall'interfaccia utente e rimuovere l'opzione "installa".

Segui questi passaggi:

1. Copiare lo snippet di Agent Installer come indicato.
2. Invece di incollare il frammento in una finestra di comando, incollalo in un editor di testo.
3. Rimuovere la parte finale "--install" (Linux) o "-install" (Windows) dal comando.
4. Copia l'intero comando dall'editor di testo.
5. Ora incollalo nella finestra dei comandi (in una directory di lavoro) ed eseguilo.

Non Windows (questi esempi sono per Kubernetes; i nomi effettivi degli script possono variare):

- Scarica e installa (predefinito):

```
 installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify && sudo -E -H ./$installerName --install
* Solo download:
```

```
installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify
```

Finestre:

- Scarica e installa (predefinito):

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify -install } else { Write-Host "Install
script checksum does not match"})"
* Solo download:
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify } else { Write-Host "Install script
checksum does not match"})"
```

Il comando di solo download scaricherà tutti gli artefatti richiesti da Data Infrastructure Insights nella directory di lavoro. Gli artefatti includono, ma non sono limitati a:

- uno script di installazione
- un file di ambiente
- un binario Telegraf
- una firma per il binario Telegraf
- un certificato pubblico per verificare la firma binaria

Il frammento di installazione scaricato e copiato da DII esegue automaticamente il checksum dello script di installazione e la firma del binario Telegraf viene verificata dallo script di installazione.

Verifica il valore del checksum

Per generare il valore di checksum, eseguire il seguente comando per la piattaforma appropriata:

- RHEL/Ubuntu:

```
 sha256sum <package_name>
* Finestre:
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Installa il pacchetto scaricato

Una volta verificati in modo soddisfacente tutti gli artefatti, è possibile avviare l'installazione dell'agente eseguendo:

Non Windows:

```
 sudo -E -H ./<installation_script_name> --install
Finestre:
```

```
.\cloudinsights-windows.ps1 -install
```

Creazione e utilizzo di token di accesso API

Per creare un token di accesso API per l'acquisizione dati Telegraf, procedere in uno dei seguenti modi:

Crea tramite la pagina di installazione di Data Collector

1. Vai alla pagina di installazione di Data Collector per la piattaforma che desideri utilizzare (Windows, Linux).
2. Crea un token con il pulsante + Token di accesso API.
3. Inserisci un nome e clicca su Salva.
4. Ora il nome del token dovrebbe essere selezionato nel menu a discesa e verrà utilizzato durante l'installazione del raccoglitore.

Crea manualmente un token di accesso API

1. Vai su Amministrazione>Accesso API.
2. Fai clic su + Token di accesso API.
3. Inserisci un nome e, facoltativamente, una descrizione.
4. In "Quali tipi di API verranno chiamate con questo token?" seleziona solo "Ingestione dati" e poi deseleziona "Unità di acquisizione".
5. In “Autorizzazioni” seleziona Lettura/Scrittura.
6. Deseleziona "Ruota automaticamente i token per Kubernetes".

Per utilizzare il token di accesso API appena creato, selezionalo dal menu a discesa "Seleziona un token di accesso API esistente o creane uno nuovo" nella pagina di installazione. Si prega di notare che possono essere utilizzati solo token con le seguenti proprietà:

- Tipo API: solo "Ingestione dati"
- Permessi: lettura/scrittura
- Rotazione automatica di Kubernetes: disattivata

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi durante la configurazione di un agente:

Problema:	Prova questo:
Dopo aver configurato un nuovo plugin e riavviato Telegraf, quest'ultimo non si avvia. I log indicano un errore simile al seguente: "[telegraf] Errore durante l'esecuzione dell'agente: Errore nel caricamento del file di configurazione /etc/telegraf/telegraf.d/cloudinsights-default.conf: output del plugin.http: riga <numero di riga>: la configurazione ha specificato i campi ["use_system_proxy"], ma non sono stati utilizzati"	La versione di Telegraf installata è obsoleta. Segui i passaggi indicati in questa pagina per **aggiornare l'agente** per la piattaforma appropriata.
Ho eseguito lo script di installazione su una vecchia installazione e ora l'agente non invia dati	Disinstallare l'agente Telegraf e quindi eseguire nuovamente lo script di installazione. Segui i passaggi **Aggiorna l'agente** indicati in questa pagina per la piattaforma appropriata.
Ho già installato un agente utilizzando Data Infrastructure Insights	Se hai già installato un agente sul tuo host/VM, non è necessario installarlo di nuovo. In questo caso, è sufficiente selezionare la piattaforma e la chiave appropriate nella schermata di installazione dell'agente e fare clic su **Continua** o **Fine**.
Ho già installato un agente, ma non tramite il programma di installazione Data Infrastructure Insights	Rimuovere l'agente precedente ed eseguire l'installazione di Data Infrastructure Insights Agent per garantire le corrette impostazioni predefinite del file di configurazione. Al termine, fare clic su **Continua** o **Fine**.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione dei raccoglitori di dati

È possibile configurare i Data Collector nel proprio ambiente Data Infrastructure Insights per raccogliere dati dai dispositivi nel data center.

Prima di iniziare

- Prima di poter iniziare a raccogliere dati, è necessario aver configurato un'unità di acquisizione.
- Sono necessarie le credenziali per i dispositivi da cui si raccolgono i dati.
- Per tutti i dispositivi da cui raccogli dati sono richiesti gli indirizzi di rete, le informazioni sull'account e le password.

Passi

1. Dal menu Data Infrastructure Insights , fare clic su **Osservabilità > Collettori**

   Il sistema visualizza i Data Collector disponibili, ordinati per fornitore.

2. Fare clic su **+ Collector** e selezionare il raccoglitore dati da configurare.

   Nella finestra di dialogo è possibile configurare il raccoglitore dati e aggiungere un'unità di acquisizione.

3. Inserisci un nome per il raccoglitore dati.

4. Fare clic su **Configurazione avanzata** per aggiungere ulteriori campi di configurazione. (Non tutti i raccoglitori di dati richiedono una configurazione avanzata.)
5. Fare clic su **Test configurazione** per verificare che il raccoglitore dati sia configurato correttamente.
6. Fare clic su **Aggiungi raccoglitore** per salvare la configurazione e aggiungere il raccoglitore dati al tenant di Data Infrastructure Insights .

Potrebbero essere necessari fino a due periodi di sondaggio prima che i dati del servizio vengano visualizzati nelle dashboard o siano disponibili per l'interrogazione.

- 1° sondaggio di inventario: immediatamente
- 1° sondaggio sui dati delle prestazioni per stabilire una linea di base: subito dopo il sondaggio dell'inventario
- 2° sondaggio sulle prestazioni: entro 15 secondi dal completamento del 1° sondaggio sulle prestazioni

Il polling procede quindi in base agli intervalli di polling dell'inventario e delle prestazioni configurati.

Determinazione dello stato di acquisizione del raccoglitore dati

Poiché i raccoglitori di dati sono la fonte primaria di informazioni per Data Infrastructure Insights, è fondamentale assicurarsi che rimangano in esecuzione.

Lo stato del raccoglitore dati viene visualizzato nell'angolo in alto a destra di qualsiasi pagina di risorsa come messaggio "Acquisito N minuti fa", dove N indica l'ora di acquisizione più recente del/i raccoglitore/i dati della risorsa. Viene visualizzata anche la data/ora di acquisizione.

Facendo clic sul messaggio viene visualizzata una tabella con il nome del raccoglitore dati, lo stato e l'ora dell'ultima acquisizione riuscita. Se hai effettuato l'accesso come amministratore, cliccando sul collegamento del nome del raccoglitore dati nella tabella verrai indirizzato alla pagina dei dettagli di quel raccoglitore dati.

Gestione dei raccoglitori di dati configurati

La pagina Data Collector installati fornisce l'accesso ai data collector configurati per Data Infrastructure Insights. È possibile utilizzare questa pagina per modificare i raccoglitori di dati esistenti.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Osservabilità > Collettori**

   Viene visualizzata la schermata Raccoglitori dati disponibili.

2. Fare clic su **Raccolta dati installati**

   Viene visualizzato un elenco di tutti i Data Collector installati. L'elenco fornisce il nome del collettore, lo stato, l'indirizzo IP a cui il collettore sta accedendo e l'ultima volta che i dati sono stati acquisiti da un dispositivo. Le azioni che possono essere eseguite in questa schermata includono:

   - Controllo dei sondaggi
   - Modifica le credenziali del raccoglitore dati
   - Clonare i collettori di dati

Controllo del polling del Data Collector

Dopo aver apportato una modifica a un raccoglitore dati, potresti voler eseguire immediatamente un polling per verificare le modifiche oppure potresti voler posticipare la raccolta dati su un raccoglitore dati per uno, tre o cinque giorni mentre lavori su un problema.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Osservabilità > Collettori**
2. Fare clic su **Raccolta dati installati**
3. Seleziona la casella di controllo a sinistra del Data Collector che desideri modificare
4. Fare clic su **Azioni in blocco** e selezionare l'azione di sondaggio che si desidera eseguire.

   È possibile eseguire azioni in blocco contemporaneamente su più Data Collector. Selezionare i raccoglitori di dati e scegliere l'azione da eseguire dal menu **Azione in blocco**.

Modifica delle informazioni del raccoglitore dati

È possibile modificare le informazioni di configurazione del raccoglitore dati esistente.

Per modificare un singolo raccoglitore di dati:

1. Nel menu Data Infrastructure Insights , fare clic su **Osservabilità > Collettori** per aprire l'elenco dei collettori dati installati.
2. Nel menu delle opzioni a destra del raccoglitore dati che vuoi modificare, clicca su **Modifica**.

   Si apre la finestra di dialogo Modifica raccoglitore.

3. Inserisci le modifiche e clicca su **Test configurazione** per testare la nuova configurazione oppure clicca su **Salva** per salvare la configurazione.

È anche possibile modificare più raccoglitori di dati:

1. Selezionare la casella di controllo a sinistra di ogni raccoglitore dati che si desidera modificare.
2. Fare clic sul pulsante **Azioni in blocco** e scegliere **Modifica** per aprire la finestra di dialogo Modifica raccoglitore dati.
3. Modificare i campi come sopra.

   I collettori di dati selezionati devono essere dello stesso fornitore e modello e risiedere nella stessa unità di acquisizione.

   Quando si modificano più raccoglitori di dati, il campo Nome raccoglitore di dati mostra "Misto" e non può essere modificato. Altri campi, come nome utente e password, risultano "Misti" e possono essere modificati. I campi che condividono lo stesso valore nei raccoglitori di dati selezionati mostrano i valori correnti e possono essere modificati.

   Quando si modificano più raccoglitori di dati, il pulsante **Configurazione di prova** non è disponibile.

Clonazione di collettori di dati

Utilizzando la funzione di clonazione, è possibile aggiungere rapidamente un'origine dati che abbia le stesse credenziali e gli stessi attributi di un'altra origine dati. La clonazione consente di configurare facilmente più

istanze dello stesso tipo di dispositivo.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Osservabilità > Collettori**.
2. Fare clic su **Raccolta dati installati**.
3. Fare clic sulla casella di controllo a sinistra del raccoglitore dati che si desidera copiare.
4. Nel menu delle opzioni a destra del raccoglitore dati selezionato, fare clic su **Clona**.

   Viene visualizzata la finestra di dialogo Clona raccolta dati.

5. Inserisci le nuove informazioni nei campi richiesti.
6. Fare clic su **Salva**.

Dopo aver finito

L'operazione di clonazione copia tutti gli altri attributi e impostazioni per creare il nuovo raccoglitore dati.

Esecuzione di azioni in blocco sui collettori di dati

È possibile modificare contemporaneamente alcune informazioni per più raccoglitori di dati. Questa funzione consente di avviare un sondaggio, posticiparlo e riprenderlo su più raccoglitori di dati. Inoltre, è possibile eliminare più raccoglitori di dati.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Osservabilità > Collettori**
2. Fare clic su **Raccolta dati installati**
3. Fare clic sulla casella di controllo a sinistra dei raccoglitori di dati che si desidera modificare.
4. Nel menu delle opzioni a destra, fare clic sull'opzione che si desidera eseguire.

Dopo aver finito

L'operazione selezionata viene eseguita sui raccoglitori di dati. Quando si sceglie di eliminare i raccoglitori di dati, viene visualizzata una finestra di dialogo che richiede di confermare l'azione.

Ricerca di un raccoglitore di dati fallito

Se un raccoglitore dati presenta un messaggio di errore e un impatto elevato o medio, è necessario analizzare il problema utilizzando la pagina di riepilogo del raccoglitore dati con le relative informazioni collegate.

Per determinare la causa del mancato funzionamento dei raccoglitori dati, attenersi alla seguente procedura. I messaggi di errore del Data Collector vengono visualizzati nel menu **Amministrazione** e nella pagina **Data Collector installati**.

Passi

1. Fare clic su **Amministrazione** > **Raccolta dati** > **Raccolta dati installati**.
2. Fare clic sul nome collegato del raccoglitore dati non riuscito per aprire la pagina Riepilogo.
3. Nella pagina Riepilogo, controlla l'area Commenti per leggere eventuali note lasciate da un altro tecnico che potrebbe stare indagando su questo guasto.
4. Annotare eventuali messaggi sulle prestazioni.

5. Sposta il puntatore del mouse sui segmenti del grafico della cronologia degli eventi per visualizzare informazioni aggiuntive.
6. Selezionare un messaggio di errore per un dispositivo visualizzato sotto la cronologia degli eventi e fare clic sull'icona Dettagli errore visualizzata a destra del messaggio.

   I dettagli dell'errore includono il testo del messaggio di errore, le cause più probabili, le informazioni in uso e i suggerimenti su cosa si può fare per correggere il problema.

7. Nell'area Dispositivi segnalati da questo raccoglitore dati, è possibile filtrare l'elenco per visualizzare solo i dispositivi di interesse e fare clic sul **Nome** collegato di un dispositivo per visualizzare la pagina delle risorse per quel dispositivo.
8. Quando torni alla pagina di riepilogo del raccoglitore dati, controlla l'area **Mostra modifiche recenti** in fondo alla pagina per verificare se le modifiche recenti potrebbero aver causato il problema.

Importazione di dashboard

Data Infrastructure Insights fornisce una serie di dashboard consigliate per ottenere informazioni aziendali sui tuoi dati. Ogni dashboard contiene widget progettati per aiutarti a rispondere a una domanda specifica o a risolvere un problema specifico rilevante per i dati attualmente raccolti sul tuo tenant. DII consente inoltre di esportare una dashboard utile e di importarla in un altro tenant.

Importazione dalla Galleria della Dashboard

Per importare una dashboard dalla galleria, procedere come segue:

1. Seleziona **Osservabilità > Esplora > Tutte le dashboard**
2. Fare clic su **+Importa dashboard** e scegliere *Importa dalla galleria*.

   Viene visualizzato un elenco di **Dashboard consigliate**, in base ai raccoglitori di dati presenti nel tuo ambiente. Sono disponibili dashboard per rispondere a domande su diversi tipi di oggetti, tra cui AWS, NetApp, Storage, VMware e altri.

3. Seleziona una o più dashboard dall'elenco e fai clic su **Aggiungi dashboard**. Queste dashboard verranno visualizzate nell'elenco delle dashboard.

Oltre alle Dashboard consigliate, puoi anche scegliere di importare **Dashboard aggiuntive** che non sono pertinenti ai tuoi dati attuali. Ad esempio, se al momento non hai installato alcun raccoglitore di dati di archiviazione ma prevedi di configurarne alcuni in futuro, puoi comunque scegliere di importare i dashboard rilevanti per l'archiviazione. Queste dashboard saranno disponibili per la visualizzazione, ma potrebbero non mostrare dati rilevanti finché non sarà configurato almeno un raccoglitore di dati di archiviazione.

L'importazione dalla galleria della dashboard è disponibile per gli utenti con ruolo di Amministratore o Proprietario dell'account.

Importazione di una dashboard esportata

Per **esportare** una dashboard, nella pagina **Osservabilità > Esplora > Tutte le dashboard**, fare clic sul menu a destra della dashboard e scegliere *Esporta*. È anche possibile selezionare più dashboard e scegliere *Esporta* dal menu a discesa *Azioni in blocco*. I dashboard vengono salvati in un file .ZIP sul sistema locale.

Per **importare** la dashboard, vai al tenant desiderato e procedi come segue:

1. Seleziona **Osservabilità > Esplora > Tutte le dashboard**
2. Fare clic su **+Importa dashboard** e scegliere *Importa da file*. Seleziona il file .ZIP del file esportato in precedenza. La/le dashboard verranno importate e verranno visualizzate nell'elenco delle dashboard. Tieni presente che se stai importando una dashboard con lo stesso nome di una dashboard esistente, al nome della dashboard verrà aggiunto un "(2)".

Account utente e ruoli

Data Infrastructure Insights fornisce fino a quattro ruoli di account utente: proprietario dell'account, amministratore, utente e ospite. A ciascun account vengono assegnati livelli di autorizzazione specifici, come indicato nella tabella seguente. Gli utenti sono entrambi"invitato" a Data Infrastructure Insights e assegnato un ruolo specifico, oppure puoi accedere tramite"Autorizzazione Single Sign-On (SSO)" con un ruolo predefinito. L'autorizzazione SSO è disponibile come funzionalità in Data Infrastructure Insights Premium Edition.

Livelli di autorizzazione

Per creare o modificare gli account utente, è necessario utilizzare un account con privilegi di amministratore. A ciascun account utente viene assegnato un ruolo per ciascuna funzionalità di Data Infrastructure Insights tra i seguenti livelli di autorizzazione.

Ruolo	Osservabilità	Sicurezza del carico di lavoro	Segnalazione	Amministratore
Titolare dell'account	Uguale all'amministratore	Uguale all'amministratore	Uguale all'amministratore	Uguale all'amministratore, gestisce anche l'autenticazione SSO e la configurazione della federazione delle identità. È inoltre possibile assegnare proprietari aggiuntivi e aggiungere clienti al tenant master del Managed Service Provider (MSP).

Ruolo	Osservabilità	Sicurezza del carico di lavoro	Segnalazione	Amministratore
Amministratore	Può eseguire tutte le funzioni di osservabilità, nonché la gestione dei collettori di dati.	Può eseguire tutte le funzioni di sicurezza, comprese quelle per avvisi, analisi forense, raccoglitori di dati, policy di risposta automatizzate e token API per la sicurezza. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di sicurezza.	Può eseguire tutte le funzioni utente/autore, inclusa la gestione dei token API di reporting, nonché tutte le attività amministrative quali la configurazione dei report e l'arresto e il riavvio delle attività di reporting. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di reporting.	È possibile invitare altri utenti ma assegnare solo ruoli di Osservabilità. È possibile visualizzare ma non modificare la configurazione SSO. Può creare e gestire token di accesso API. Può visualizzare le informazioni di audit. È possibile visualizzare informazioni sull'abbonamento, sull'utilizzo e sulla cronologia. Può gestire gli elenchi dei destinatari delle notifiche di avviso globali e delle notifiche di abbonamento.
Utente	Può visualizzare e modificare dashboard, query, avvisi, annotazioni, regole di annotazione e applicazioni, nonché gestire la risoluzione dei dispositivi.	Può visualizzare e gestire gli avvisi e visualizzare le analisi forensi. Il ruolo utente può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot e gestire l'accesso limitato dell'utente.	Può eseguire tutte le funzioni di Ospite/Consumatore , nonché creare e gestire report e dashboard.	Non disponibile

Ruolo	Osservabilità	Sicurezza del carico di lavoro	Segnalazione	Amministratore
Ospite	Ha accesso in sola lettura alle pagine delle risorse, alle dashboard, agli avvisi e può visualizzare ed eseguire query.	È possibile visualizzare avvisi e analisi forensi. Il ruolo ospite non può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot o limitare l'accesso degli utenti.	È possibile visualizzare, pianificare ed eseguire report e impostare preferenze personali, come quelle relative a lingue e fusi orari. Gli ospiti/consumatori non possono creare report o eseguire attività amministrative.	Non disponibile

La prassi migliore è limitare il numero di utenti con autorizzazioni di amministratore. Il maggior numero di account dovrebbe essere costituito da account utente o ospiti.

Autorizzazioni Data Infrastructure Insights per ruolo utente

Nella tabella seguente sono riportate le autorizzazioni Data Infrastructure Insights concesse a ciascun ruolo utente.

Caratteristica	Amministratore/Proprietario dell'account	Utente	Ospite
Unità di acquisizione: Aggiungi/Modifica/Elimina	E	N	N
Avvisi*: Crea/Modifica/Elimina	E	E	N
Avvisi*: Visualizza	E	E	E
Regole di annotazione: Crea/Esegui/Modifica/Elimina	E	E	N
Annotazioni: Crea/Modifica/Assegna/Visualizza/Rimuovi/Elimina	E	E	N
Accesso API*: Crea/Rinomina/Disabilita/Revoca	E	N	N
Applicazioni: Crea/Visualizza/Modifica/Elimina	E	E	N
Pagine delle risorse: modifica	E	E	N

Pagine delle risorse: Visualizza	E	E	E
Audit: Visualizza	E	N	N
Costo del cloud	E	N	N
Sicurezza	E	N	N
Dashboard: Crea/Modifica/Elimina	E	E	N
Dashboard: Visualizza	E	E	E
Raccoglitori di dati: Aggiungi/Modifica/Sondaggio/Elimina	E	N	N
Notifiche: Visualizza	E	E	E
Notifiche: Modifica	E	N	N
Query: Crea/Modifica/Elimina	E	E	N
Query: Visualizza/Esegui	E	E	E
Risoluzione del dispositivo	E	E	N
Report*: Visualizza/Esegui	E	E	E
Report*: Crea/Modifica/Elimina/Pianifica	E	E	N
Abbonamento: Visualizza/Modifica	E	N	N
Gestione utenti: Invita/Aggiungi/Modifica/Disattiva	E	N	N

*Richiede l'edizione Premium

Creazione di account invitando utenti

La creazione di un nuovo account utente avviene tramite NetApp Console. Un utente può rispondere all'invito inviato tramite e-mail, ma se non ha un account con Console, deve registrarsi per poter accettare l'invito.

Prima di iniziare

- Il nome utente è l'indirizzo email dell'invito.
- Comprendi i ruoli utente che assegnerai.
- Le password vengono definite dall'utente durante la procedura di registrazione.

Passi

1. Accedi a Data Infrastructure Insights
2. Nel menu, fare clic su **Amministrazione > Gestione utenti**

Viene visualizzata la schermata Gestione utenti. La schermata contiene un elenco di tutti gli account presenti nel sistema.

3. Clicca **+ Utente**

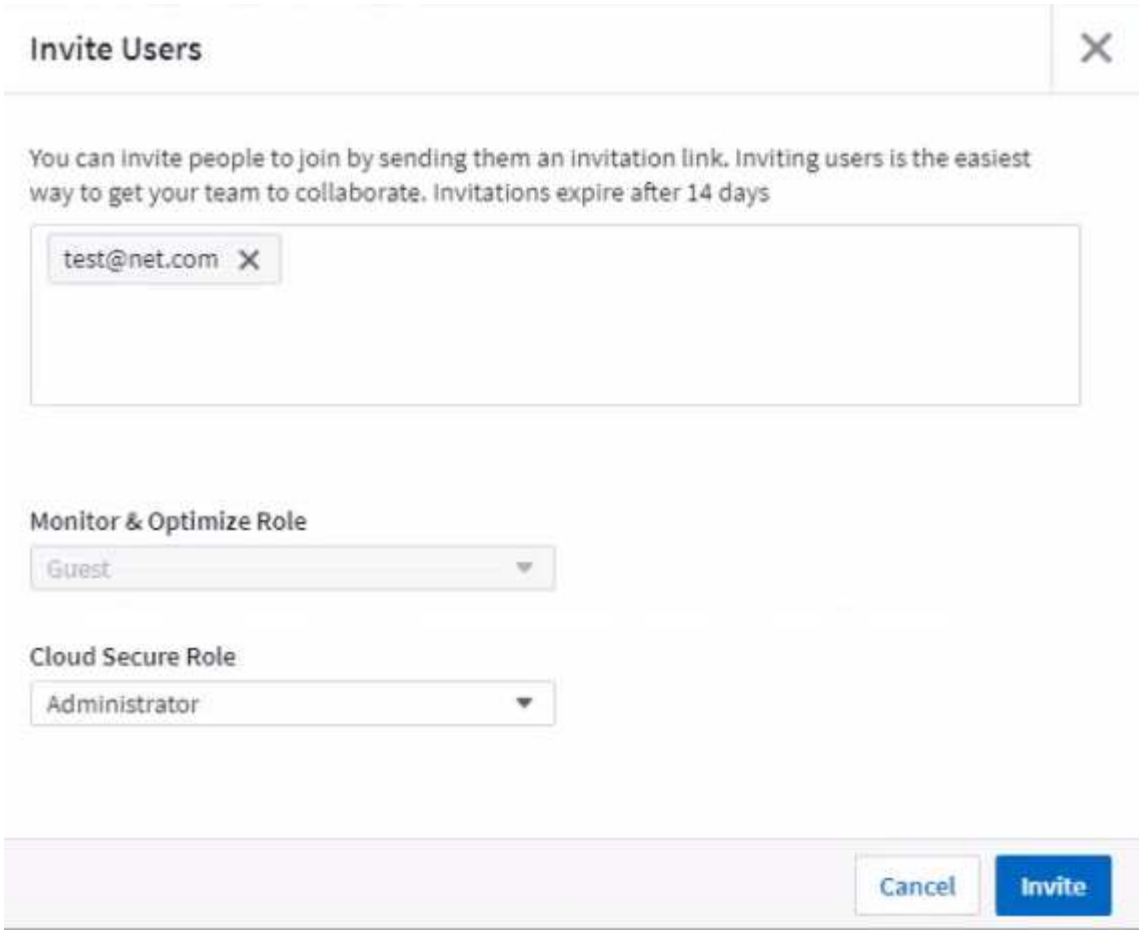
   Viene visualizzata la schermata **Invita utente**.

4. Inserisci uno o più indirizzi email per gli inviti.

   Nota: quando si inseriscono più indirizzi, vengono tutti creati con lo stesso ruolo. È possibile assegnare lo stesso ruolo a più utenti.

5. Selezionare il ruolo dell'utente per ciascuna funzionalità di Data Infrastructure Insights.

   Le funzionalità e i ruoli tra cui puoi scegliere dipendono dalle funzionalità a cui hai accesso nel tuo specifico ruolo di amministratore. Ad esempio, se si dispone del ruolo di amministratore solo per la creazione di report, sarà possibile assegnare agli utenti qualsiasi ruolo nella creazione di report, ma non sarà possibile assegnare ruoli per l'osservabilità o la sicurezza.



6. Fai clic su **Invita**

   L'invito viene inviato all'utente. Gli utenti avranno 14 giorni per accettare l'invito. Una volta accettato l'invito, l'utente verrà indirizzato al NetApp Cloud Portal, dove potrà registrarsi utilizzando l'indirizzo e-mail presente nell'invito. Se hanno già un account associato a quell'indirizzo e-mail, possono semplicemente effettuare l'accesso e potranno quindi accedere al loro ambiente Data Infrastructure Insights .

Modifica del ruolo di un utente esistente

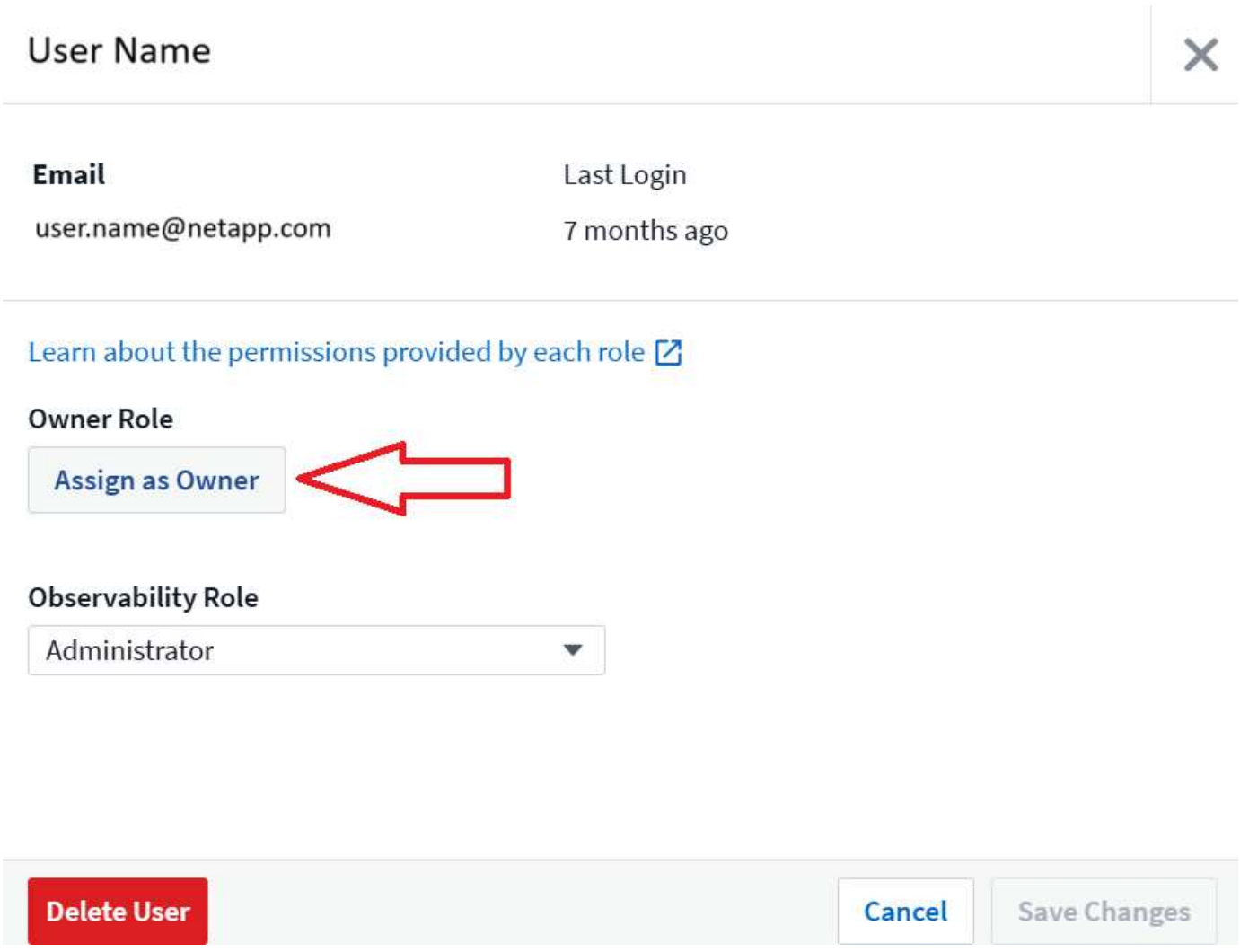
Per modificare il ruolo di un utente esistente, inclusa l'aggiunta come **proprietario secondario dell'account**, segui questi passaggi.

1. Fare clic su **Amministrazione > Gestione utenti**. Nella schermata viene visualizzato un elenco di tutti gli account presenti nel sistema.
2. Fare clic sul nome utente dell'account che si desidera modificare.
3. Modificare il ruolo dell'utente in ogni set di funzionalità Data Infrastructure Insights in base alle esigenze.
4. Fare clic su *Salva modifiche*.

Per assegnare un proprietario di account secondario

Per poter assegnare il ruolo di proprietario dell'account a un altro utente, è necessario aver effettuato l'accesso come proprietario dell'account per Observability.

1. Fare clic su **Amministrazione > Gestione utenti**.
2. Fare clic sul nome utente dell'account che si desidera modificare.
3. Nella finestra di dialogo Utente, fare clic su **Assegna come proprietario**.
4. Salva le modifiche.



Puoi avere tutti i proprietari di account che desideri, ma la prassi migliore è limitare il ruolo di proprietario solo a persone selezionate.

Eliminazione degli utenti

Un utente con il ruolo di amministratore può eliminare un utente (ad esempio, qualcuno che non fa più parte dell'azienda) facendo clic sul nome dell'utente e poi su *Elimina utente* nella finestra di dialogo. L'utente verrà rimosso dall'ambiente Data Infrastructure Insights .

Tieni presente che tutte le dashboard, le query, ecc. create dall'utente rimarranno disponibili nell'ambiente Data Infrastructure Insights anche dopo la rimozione dell'utente.

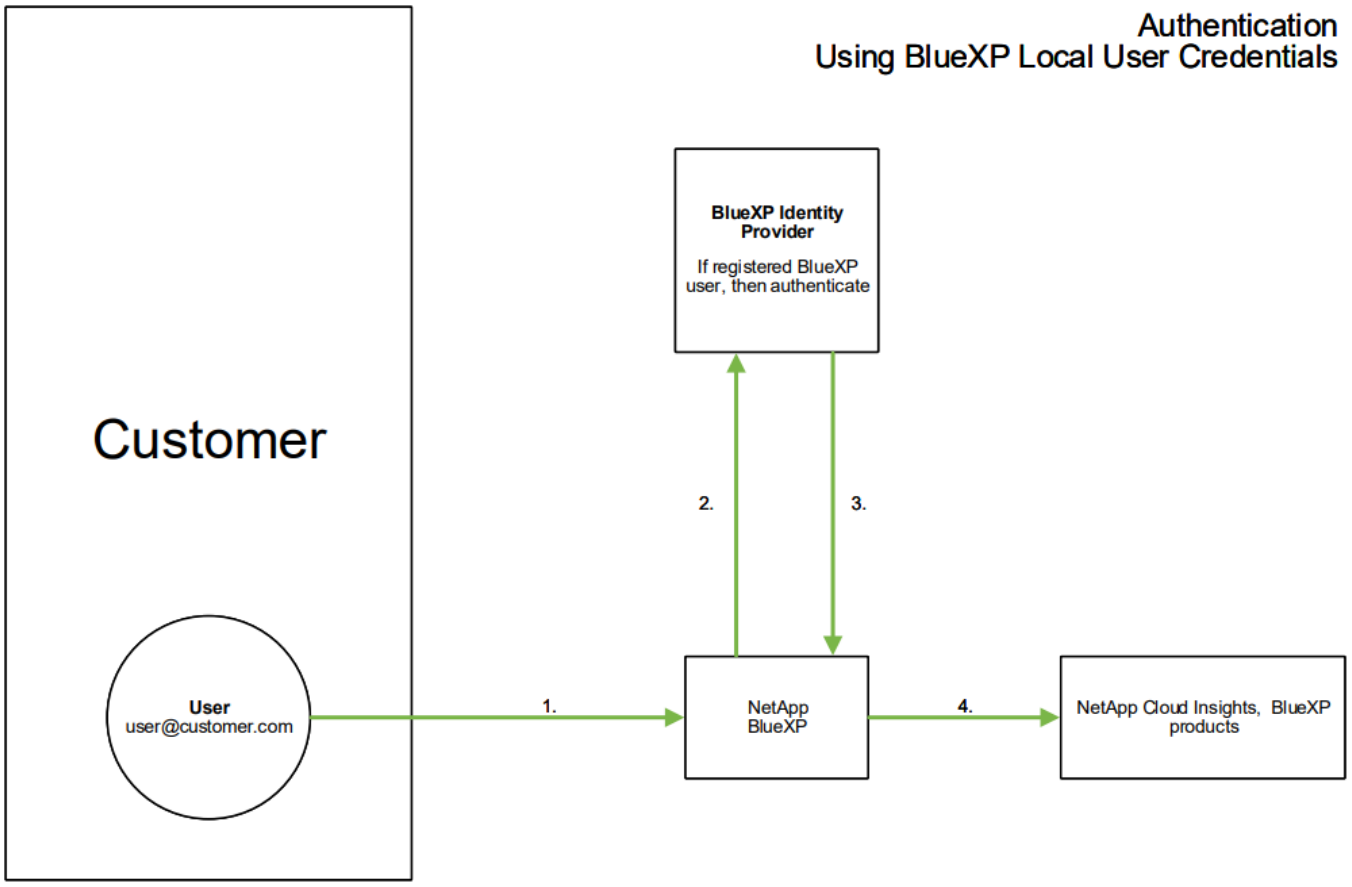
Single Sign-On (SSO) e federazione delle identità

Che cos'è la federazione delle identità?

Con la Federazione delle Identità:

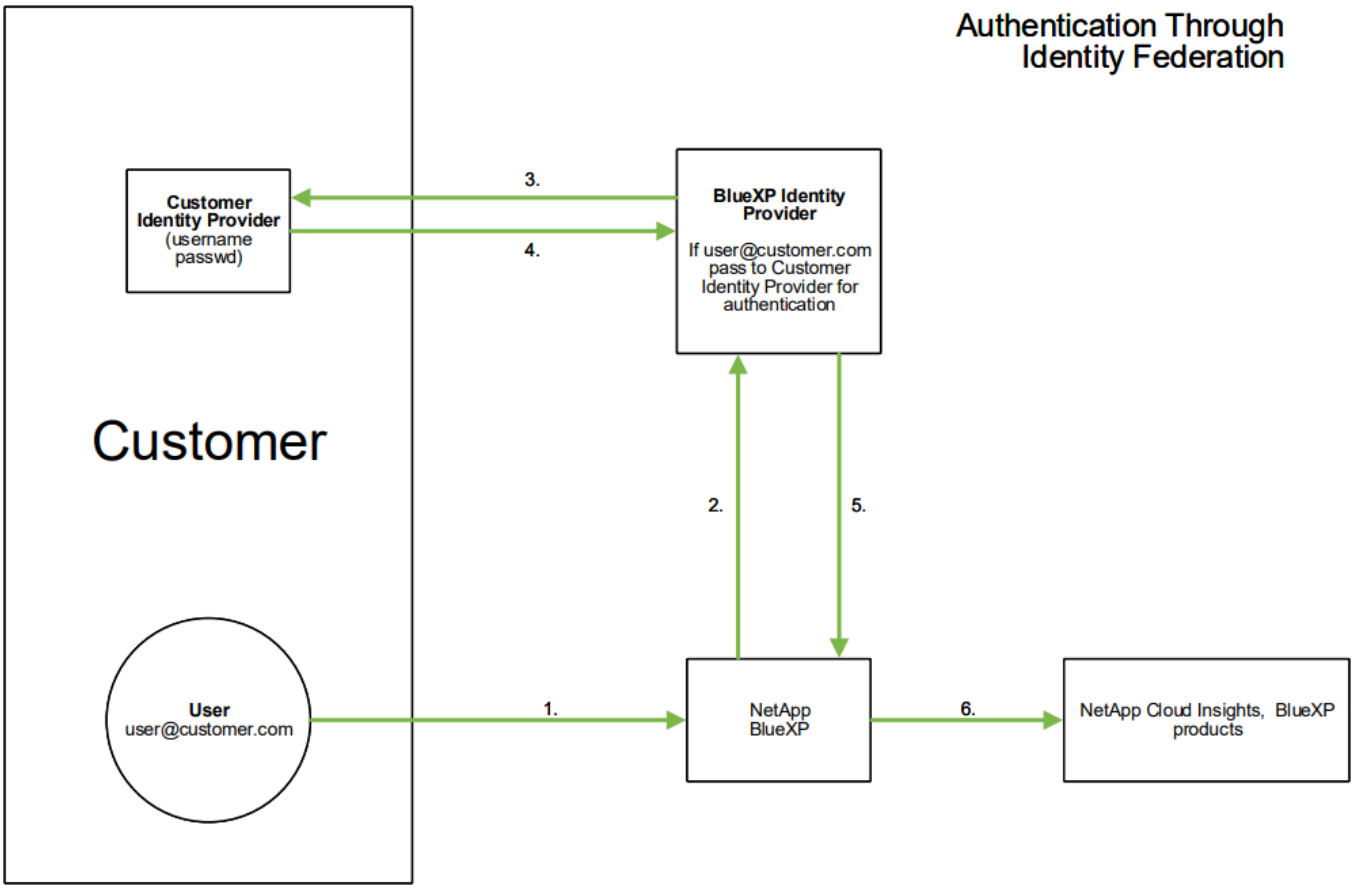
- L'autenticazione è delegata al sistema di gestione dell'identità del cliente, utilizzando le credenziali del cliente dalla directory aziendale e criteri di automazione come l'autenticazione a più fattori (MFA).
- Gli utenti accedono una sola volta a tutti i servizi NetApp Console (Single Sign On).

Gli account utente vengono gestiti nella NetApp Console per tutti i servizi cloud. Per impostazione predefinita, l'autenticazione viene eseguita tramite un profilo utente locale della console. Di seguito è riportata una panoramica semplificata di tale processo:



Tuttavia, alcuni clienti preferiscono utilizzare il proprio provider di identità per autenticare gli utenti per Data Infrastructure Insights e gli altri servizi NetApp Console . Con Identity Federation, gli account NetApp Console vengono autenticati utilizzando le credenziali della directory aziendale.

Di seguito è riportato un esempio semplificato di tale processo:



Nel diagramma soprastante, quando un utente accede a Data Infrastructure Insights, viene indirizzato al sistema di gestione delle identità del cliente per l'autenticazione. Una volta autenticato l'account, l'utente viene indirizzato all'URL del tenant Data Infrastructure Insights .

Abilitazione della federazione delle identità

La console utilizza Auth0 per implementare la federazione delle identità e integrarsi con servizi quali Active Directory Federation Services (ADFS) e Microsoft Azure Active Directory (AD). Per configurare la federazione delle identità, vedere"Istruzioni della Federazione" .

> È necessario configurare Identity Federation prima di poter utilizzare SSO con Data Infrastructure Insights.

È importante comprendere che la modifica della federazione delle identità non si applicherà solo a Data Infrastructure Insights, ma a tutti i NetApp Console Services. Il cliente deve discutere questa modifica con il team NetApp di ciascun prodotto di cui è in possesso, per assicurarsi che la configurazione utilizzata funzioni con Identity Federation o se è necessario apportare modifiche a qualche account. Il cliente dovrà coinvolgere anche il proprio team SSO interno nel passaggio alla federazione delle identità.

È inoltre importante rendersi conto che, una volta abilitata la federazione delle identità, qualsiasi modifica al provider di identità dell'azienda (ad esempio il passaggio da SAML a Microsoft AD) richiederà probabilmente

risoluzione dei problemi/modifiche/attenzione per aggiornare i profili degli utenti.

Per questo o altri problemi relativi alla federazione, puoi aprire un ticket di supporto a https://mysupport.netapp.com/site/help .

Provisioning automatico degli utenti Single Sign-On (SSO)

Oltre a invitare gli utenti, gli amministratori possono abilitare l'accesso **Single Sign-On (SSO) User Auto-Provisioning** a Data Infrastructure Insights per tutti gli utenti nel loro dominio aziendale, senza doverli invitare individualmente. Con l'SSO abilitato, qualsiasi utente con lo stesso indirizzo email di dominio può accedere a Data Infrastructure Insights utilizzando le proprie credenziali aziendali.

> *SSO User Auto-Provisioning* è disponibile in Data Infrastructure Insights Premium Edition e deve essere configurato prima di poter essere abilitato per Data Infrastructure Insights. La configurazione del provisioning automatico dell'utente SSO include"Federazione di identità" tramite NetApp Console come descritto nella sezione precedente. La federazione consente agli utenti con accesso Single Sign-On di accedere agli account NetApp Console utilizzando le credenziali della directory aziendale, avvalendosi di standard aperti quali Security Assertion Markup Language 2.0 (SAML) e OpenID Connect (OIDC).

Per configurare *SSO User Auto-Provisioning*, nella pagina **Amministrazione > Gestione utenti**, è necessario prima aver configurato la federazione delle identità. Selezionare il collegamento **Imposta federazione** nel banner per procedere alla Federazione della console. Una volta configurata, gli amministratori di Data Infrastructure Insights possono abilitare l'accesso utente SSO. Quando un amministratore abilita il provisioning automatico degli utenti SSO, sceglie un ruolo predefinito per tutti gli utenti SSO (ad esempio Ospite o Utente). Gli utenti che accedono tramite SSO avranno quel ruolo predefinito.

Talvolta, un amministratore potrebbe voler promuovere un singolo utente dal ruolo SSO predefinito (ad esempio, per renderlo amministratore). Possono farlo nella pagina **Amministrazione > Gestione utenti** cliccando sul menu a destra dell'utente e selezionando *Assegna ruolo*. Gli utenti a cui viene assegnato un ruolo esplicito in questo modo continuano ad avere accesso a Data Infrastructure Insights anche se *SSO User Auto-Provisioning* viene successivamente disabilitato.

Se l'utente non necessita più del ruolo elevato, è possibile fare clic sul menu per *Rimuovi utente*. L'utente verrà rimosso dall'elenco. Se è abilitato *SSO User Auto-Provisioning*, l'utente può continuare ad accedere a Data Infrastructure Insights tramite SSO, con il ruolo predefinito.

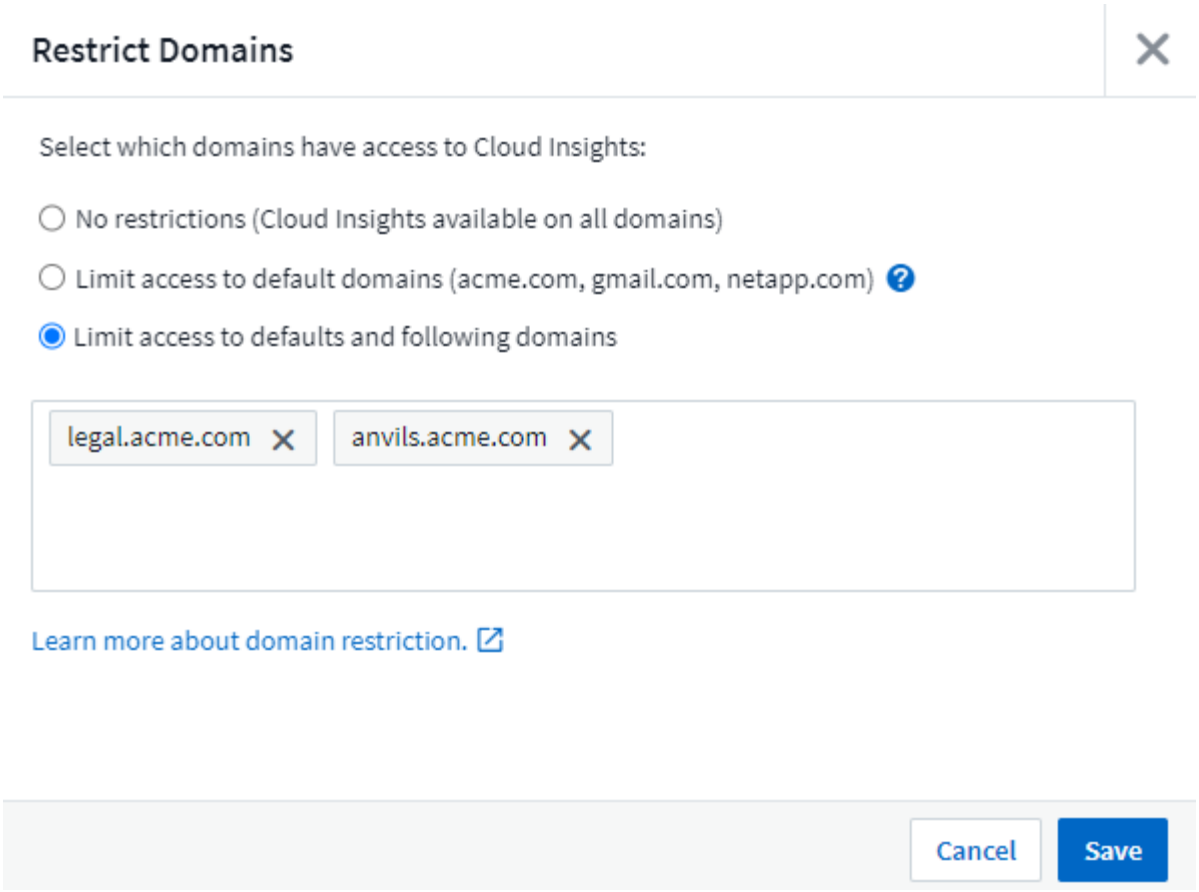
Puoi scegliere di nascondere gli utenti SSO deselezionando la casella di controllo **Mostra utenti SSO**.

Tuttavia, non abilitare *SSO User Auto-Provisioning* se una delle seguenti condizioni è vera:

- La tua organizzazione ha più di un tenant Data Infrastructure Insights
- La tua organizzazione non desidera che alcun utente nel dominio federato abbia un certo livello di accesso automatico al tenant di Data Infrastructure Insights . *Al momento, non abbiamo la possibilità di utilizzare i gruppi per controllare l'accesso ai ruoli con questa opzione*.

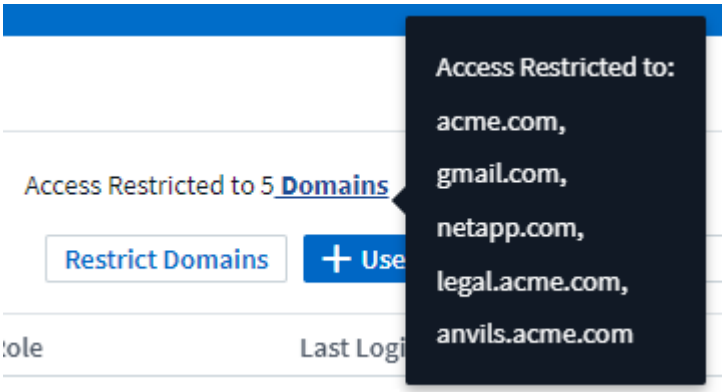
Limitazione dell'accesso per dominio

Data Infrastructure Insights può limitare l'accesso degli utenti solo ai domini specificati. Nella pagina **Amministrazione > Gestione utenti**, seleziona "Limita domini".



Ti vengono presentate queste scelte:

- Nessuna restrizione: Data Infrastructure Insights rimane accessibile agli utenti indipendentemente dal loro dominio.
- Limita l'accesso ai domini predefiniti: i domini predefiniti sono quelli utilizzati dai proprietari dell'account dell'ambiente Data Infrastructure Insights . Questi domini sono sempre accessibili.
- Limita l'accesso ai valori predefiniti e ai domini specificati. Elenca tutti i domini a cui desideri che abbiano accesso al tuo ambiente Data Infrastructure Insights , oltre ai domini predefiniti.



Elenco di riferimento del Data Collector di Data Infrastructure Insights

Data Infrastructure Insights supporta una varietà di Data Collector di numerosi fornitori e servizi.

I raccoglitori di dati sono classificati in base a queste tipologie:

- Infrastruttura: acquisita da dispositivi del fornitore quali array di archiviazione, switch, hypervisor o dispositivi di backup.
- Servizio: acquisito da servizi come Kubernetes o Docker. Chiamato anche *Integrazione*.

Elenco alfabetico dei Data Collector supportati da Data Infrastructure Insights:

Responsabile della raccolta dati	Tipo
"Amazon EC2 ed EBS"	Infrastruttura
"AWS S3 come storage"	Infrastruttura
"Amazon FSx for NetApp ONTAP"	Infrastruttura
"Apache"	Servizio
"Azure NetApp Files"	Infrastruttura
"Macchine virtuali e VHD di Azure"	Infrastruttura
"Consulente di rete Brocade (BNA)"	Infrastruttura
"Switch Fibre Channel Brocade"	Infrastruttura
"Brocade FOS REST"	Infrastruttura
"Switch Cisco MDS Fabric"	Infrastruttura
"Console"	Servizio
"Couchbase"	Servizio
"CouchDB"	Servizio
"Cohesity SmartFiles"	Infrastruttura
"Dominio dati Dell EMC"	Infrastruttura
"Dell EMC ECS"	Infrastruttura
"Dell EMC PowerScale (in precedenza Isilon)"	Infrastruttura
"Dell EMC Isilon / PowerScale REST"	Infrastruttura
"Dell EMC PowerStore"	Infrastruttura
"Dell EMC Recoverpoint"	Infrastruttura
"Dell EMC ScaleIO/PowerFlex"	Infrastruttura
"Dell EMC Unity"	Infrastruttura
"Dell EMC Unisphere REST"	Infrastruttura

Responsabile della raccolta dati	Tipo
"Famiglia di dispositivi Dell EMC VMAX/PowerMax"	Infrastruttura
"Storage a blocchi Dell EMC VNX"	Infrastruttura
"File Dell EMC VNX"	Infrastruttura
"Dell EMC VNX Unified"	Infrastruttura
"Dell EMC VPLEX"	Infrastruttura
"Dell EMC XtremIO"	Infrastruttura
"Serie Dell XC"	Infrastruttura
"Docker"	Servizio
"Elasticsearch"	Servizio
"Flink"	Servizio
"Fujitsu ETERNUS DX"	Infrastruttura
"Google Compute e Storage"	Infrastruttura
"Google Cloud NetApp Volumes"	Infrastruttura
"Hadoop"	Servizio
"HAProxy"	Servizio
"Piattaforma di contenuti Hitachi (HCP)"	Infrastruttura
"Suite di comando Hitachi Vantara"	Infrastruttura
"Piattaforma NAS Hitachi Vantara"	Infrastruttura
"Centro operativo Hitachi"	Infrastruttura
"Storage HP Enterprise Alletra 6000 (in precedenza Nimble)"	Infrastruttura
"Archiviazione HP Enterprise Alletra 9000 / Primera (in precedenza 3PAR)"	Infrastruttura
"HP Enterprise Command View"	Infrastruttura
"Dispositivi Huawei OceanStor e Dorado"	Infrastruttura
"IBM Cleversafe"	Infrastruttura
"Serie IBM CS"	Infrastruttura
"Controller del volume IBM SAN (SVC)"	Infrastruttura
"IBM System Storage serie DS8000"	Infrastruttura
"Archiviazione IBM XIV e A9000"	Infrastruttura
"Infinidat InfiniBox"	Infrastruttura
"Giava"	Servizio
"Kafka"	Servizio
"Condensatore"	Servizio

Responsabile della raccolta dati	Tipo
"Kibana"	Servizio
"Kubernetes"	Servizio
"Serie Lenovo HX"	Infrastruttura
"Memcached"	Servizio
"Azure NetApp Files"	Infrastruttura
"Microsoft Hyper-V"	Infrastruttura
"MongoDB"	Servizio
"MySQL"	Servizio
"NetApp Cloud Volumes ONTAP"	Infrastruttura
"Connessione NetApp Cloud per ONTAP 9.9+"	Infrastruttura
"NetApp Data ONTAP 7-Mode"	Infrastruttura
"NetApp E-Series"	Infrastruttura
"NetApp E-Series REST"	Infrastruttura
"Amazon FSx for NetApp ONTAP"	Infrastruttura
"Centro virtuale NetApp HCI"	Infrastruttura
"Software di gestione dati NetApp ONTAP"	Infrastruttura
"Raccoglitore REST NetApp ONTAP"	Infrastruttura
"NetApp ONTAP AFX"	Infrastruttura
"Raccoglitore NetApp ONTAP ASA r2 (All-SAN Array)"	Infrastruttura
"ONTAP Select NetApp ONTAP"	Infrastruttura
"Array NetApp SolidFire All-Flash"	Infrastruttura
"NetApp StorageGRID"	Infrastruttura
"Netstat"	Servizio
"Nginx"	Servizio
"Nodo"	Servizio
"Serie Nutanix NX"	Infrastruttura
"OpenZFS"	Servizio
"Dispositivo di archiviazione Oracle ZFS"	Infrastruttura
"PostgreSQL"	Servizio
"Agente burattino"	Servizio
"Pure Storage FlashArray"	Infrastruttura
"Virtualizzazione Red Hat"	Infrastruttura
"Redis"	Servizio

Responsabile della raccolta dati	Tipo
"Ripensare DB"	Servizio
"RHEL e CentOS"	Servizio
"Archiviazione CDM di Rubrik"	Infrastruttura
"Ubuntu e Debian"	Servizio
"VAST DataStore"	Infrastruttura
"VMware vSphere"	Infrastruttura
"Finestre"	Servizio
"Guardiano dello Zoo"	Servizio

Iscrizione a Data Infrastructure Insights

Per iniziare a utilizzare Data Infrastructure Insights bastano tre semplici passaggi:

1. Registrati per un account su"* NetApp Console*" per accedere a tutte le offerte Cloud di NetApp.
2. Registrati per una prova gratuita di Data Infrastructure Insights per esplorare le funzionalità disponibili. Per registrarsi per una prova gratuita:
   - Vai a https://netapp.com
   - Seleziona **Come acquistare** nella parte superiore della pagina.
   - Seleziona **Richiedi prova**. Se non sei ancora registrato su Console, inserisci i tuoi dati e registrati. Altrimenti, accedi.
   - Fissa un appuntamento o attendi che un rappresentante ti contatti in merito alla tua prova.
3. **Iscriviti** a Data Infrastructure Insights per un accesso continuo e ininterrotto ai tuoi dati tramite una varietà di opzioni di abbonamento flessibili:
   - "Vendite dirette NetApp"
   - AWS Marketplace:
     - "Abbonamento a tempo determinato"
     - "Abbonamento a consumo"
     - "Abbonamento base fisso + pagamento in base al consumo per eccedenze"
   - "Azure Marketplace"(tutte le opzioni di abbonamento)

Durante la procedura di registrazione, puoi scegliere la regione globale in cui ospitare il tuo ambiente Data Infrastructure Insights . Per ulteriori informazioni, leggi Data Infrastructure Insights"Informazioni e Regione" .

Per informazioni dettagliate sulle funzionalità e le opzioni di prezzo Data Infrastructure Insights , vedere"Edizioni di Data Infrastructure Insights" pagina.

Durante l'utilizzo di Data Infrastructure Insights, se vedi un'icona a forma di lucchetto significa che la funzionalità non è disponibile nel tuo abbonamento attuale o è disponibile in forma limitata. Per avere accesso completo, abbonati a questa funzionalità. Alcune funzionalità sono disponibili comeValutazione del modulo prima di abbonarti.

Edizione di prova

Quando ti registri a Data Infrastructure Insights e il tuo ambiente è attivo, inizi una prova gratuita di Data Infrastructure Insights della durata di 30 giorni. Durante questa prova potrai esplorare le funzionalità offerte da Data Infrastructure Insights nel tuo ambiente.

In qualsiasi momento durante il periodo di prova, puoi abbonarti a Data Infrastructure Insights. L'abbonamento a Data Infrastructure Insights garantisce un accesso ininterrotto ai tuoi dati e un'estensione**"supporto prodotto"** opzioni.

Data Infrastructure Insights visualizza un banner quando il periodo di prova gratuito sta per scadere. All'interno del banner è presente un link *Visualizza abbonamento*, che apre la pagina **Amministrazione → Abbonamento**. Gli utenti non amministratori vedranno il banner ma non potranno accedere alla pagina Abbonamento.

Se hai bisogno di più tempo per valutare Data Infrastructure Insights e la tua prova gratuita scade tra 4 giorni o meno, puoi estenderla per altri 30 giorni. È possibile estendere il periodo di prova solo una volta. Non è possibile estendere il periodo di prova se è scaduto.

Prova tramite AWS Marketplace

Puoi anche registrarti per una prova gratuita tramite AWS Marketplace. La prova gratuita di AWS Marketplace ti dà accesso a Data Infrastructure Insights per un periodo di prova di 33 giorni.

La prova gratuita di AWS Marketplace non può essere estesa.

Cosa succede se il mio periodo di prova è scaduto?

Se la prova gratuita è scaduta e non ti sei ancora abbonato a Data Infrastructure Insights, avrai a disposizione funzionalità limitate finché non ti abbonerai. L'acquisizione dei dati potrebbe cessare e, dopo alcune settimane, i tuoi dati verranno eliminati in base alla nostra politica di conservazione dei dati.

Cosa succede se il mio abbonamento è scaduto?

Se hai un abbonamento a Data Infrastructure Insights, ma è scaduto, avrai un periodo di grazia di cinque giorni per rinnovarlo. Tutte le funzionalità di Data Infrastructure Insights rimarranno attive durante questo periodo di tolleranza.

Una volta trascorso il periodo di tolleranza, la funzionalità Data Infrastructure Insights verrà sospesa fino al rinnovo. Per rinnovare, consulta la pagina **Amministrazione > Abbonamento** oppure contatta il reparto vendite NetApp .

I dati Data Infrastructure Insights rimangono intatti per 30 giorni dopo il periodo di tolleranza. Se rinnovi l'abbonamento entro questo periodo, tutti i tuoi dati fino alla scadenza del periodo di grazia saranno disponibili.

Valutazione del modulo

Puoi anche usufruire delle **Valutazioni dei moduli**. Ad esempio, se sei già abbonato a Infrastructure Observability ma stai aggiungendo Kubernetes al tuo ambiente, entrerai automaticamente in una valutazione di Kubernetes Observability di 30 giorni, a partire dal momento in cui installi NetApp Kubernetes Monitoring Operator. Al termine del periodo di valutazione ti verrà addebitato solo l'utilizzo dell'unità gestita da Kubernetes Observability.

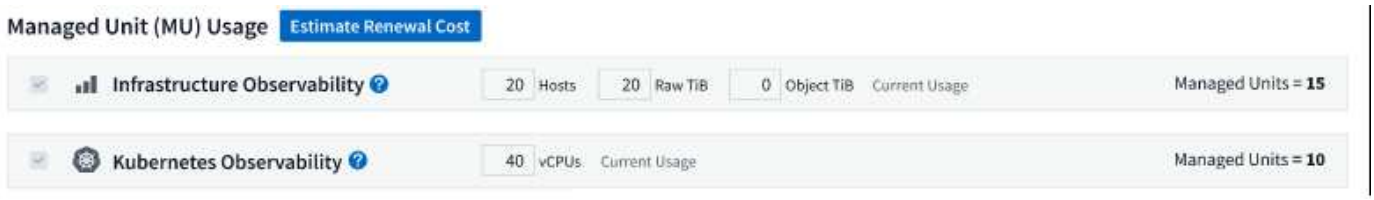
Tieni presente che ti verrà addebitato l'utilizzo della nuova unità gestita (MU) in seguito alla valutazione, quindi assicurati di pianificare di conseguenza. Al termine della valutazione del modulo, verrai avvisato se sarà necessario aggiungere altre MU per evitare l'interruzione del servizio.

Puoi monitorare l'utilizzo delle tue unità gestite nella pagina **Amministrazione > Abbonamento** nella scheda **Utilizzo**.

Una *Valutazione del modulo* non è una *Prova*: utilizziamo il termine prova quando forniamo ai clienti un periodo di prova gratuito per utilizzare il servizio Data Infrastructure Insights per confermare l'idoneità e consentire l'acquisto. La valutazione di un modulo è diversa: in questo caso consentiamo a un cliente pagante di provare un modulo di Data Infrastructure Insights che non ha utilizzato negli ultimi mesi del suo abbonamento a pagamento. Quando la valutazione è attiva, non vengono addebitati costi per il solo modulo appena configurato. L'ambiente di lavoro dei clienti è ancora in abbonamento e non è tornato alla versione di prova gratuita. L'abbonamento non è cambiato.

Estimatore

Durante la valutazione di un modulo, non ti verrà addebitato l'utilizzo di MU per le risorse consumate per il modulo, ma puoi aprire lo **Stimatore** (nella scheda *Riepilogo*) per vedere come verranno addebitate le MU dopo la valutazione, nonché provare scenari "Cosa succederebbe se" con il numero di MU di cui potresti aver bisogno in futuro. Reimposta i numeri uscendo dallo Stimatore.



Selezionare la casella di controllo accanto a un modulo per aggiungere o rimuovere tutte le MU del modulo dal costo stimato.

Lo strumento di stima ti consente anche di vedere come si sommano i numeri per un componente aggiuntivo, con cui mantieni il termine di abbonamento attuale e aumenti il numero di unità gestite con licenza, o per un'opzione di rinnovo per l'abbonamento di rinnovo che acquisteresti al termine del termine di abbonamento attuale.

Si noti che i clienti hanno diritto a una sola valutazione del modulo per abbonamento.

Opzioni di abbonamento

Per abbonarti, vai su **Amministrazione** → **Abbonamento**. Oltre ai pulsanti **Iscriviti**, potrai visualizzare i tuoi collettori dati installati e calcolare la tua misurazione stimata. Per un ambiente tipico, puoi fare clic sul pulsante self-service AWS Marketplace. Se il tuo ambiente include o si prevede che includa 1.000 o più unità gestite, hai diritto ai prezzi basati sul volume.

Misurazione dell'osservabilità

L'osservabilità Data Infrastructure Insights viene misurata in uno dei due modi seguenti:

- Misurazione della capacità
- Misurazione delle unità gestite (legacy)

Il tuo abbonamento verrà calcolato tramite uno di questi metodi, a seconda che tu abbia già un abbonamento o che tu stia lanciando un nuovo abbonamento.

Misurazione della capacità

Data Infrastructure Insights L'osservabilità misura l'utilizzo in base al livello di archiviazione del tenant. Potresti avere magazzini che rientrano in una o più di queste categorie:

- Materie prime primarie
- Oggetto grezzo
- Cloud consumato

Ogni livello viene misurato a una tariffa diversa, e il totale viene calcolato insieme per darti un diritto ponderato. La formula per calcolare l'utilizzo ponderato è la seguente:

```
 Weighted Capacity = Raw TiB + (0.1 x Object Tier Raw TiB) + (0.25 x Cloud
Tier Provisioned TiB)
Per facilitare questa operazione, DII calcola un singolo numero di
*diritto ponderato* in base alle quantità _sottoscritte_; calcola quindi
lo stesso numero in base allo spazio di archiviazione _scoperto_ e
dichiara la violazione solo se la capacità scoperta è maggiore del diritto
ponderato.  Ciò offre la flessibilità di monitorare quantità che variano
rispetto agli importi sottoscritti per ciascun livello, cosa consentita da
DII a condizione che lo spazio di archiviazione totale scoperto rientri
nell'autorizzazione ponderata sottoscritta.
```

Misurazione delle unità gestite (legacy)

Utilizzo del misuratore di osservabilità dell'infrastruttura Data Infrastructure Insights e dell'osservabilità di Kubernetes per **unità gestita**. L'utilizzo delle unità gestite viene calcolato in base al numero di **host o macchine virtuali** e alla quantità di **capacità non formattata** gestita nell'ambiente infrastrutturale.

- 1 unità gestita = 2 host (qualsiasi macchina virtuale o fisica)
- 1 unità gestita = 4 TiB di capacità non formattata di dischi fisici o virtuali

- 1 unità gestita = 40 TiB di capacità non formattata di storage secondario selezionato: AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Dell EMC ECS, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik.
- 1 unità gestita = 4 vCPU di Kubernetes.
  - 1 Regolazione K8s dell'unità gestita = 2 nodi o host monitorati anche dall'infrastruttura.

Misurazione della sicurezza del carico di lavoro

La sicurezza del carico di lavoro viene misurata dal cluster utilizzando lo stesso approccio della misurazione dell'osservabilità.

Puoi visualizzare l'utilizzo di Workload Security nella pagina **Amministrazione > Abbonamento** nella scheda **Workload Security**.

Gli abbonamenti Workload Security esistenti hanno l'utilizzo di MU regolato in modo che l'utilizzo dei nodi non consumi unità gestite. Data Infrastructure Insights misura l'utilizzo per garantire la conformità con l'utilizzo concesso in licenza.

Come posso abbonarmi?

Se il numero delle tue unità gestite è inferiore a 1.000, puoi abbonarti tramite NetApp Sales oppureauto-iscrizione tramite AWS Marketplace.

Iscriviti tramite NetApp Sales Direct

Se il numero previsto di unità gestite è pari o superiore a 1.000, fare clic su**"Contatta il reparto vendite"** pulsante per iscriverti tramite il team vendite NetApp .

Devi fornire il **numero di serie** di Data Infrastructure Insights al tuo rappresentante commerciale NetApp affinché l'abbonamento a pagamento possa essere applicato al tuo ambiente Data Infrastructure Insights . Il numero di serie identifica in modo univoco l'ambiente di prova Data Infrastructure Insights e può essere trovato nella pagina **Amministrazione > Abbonamento**.

Auto-iscrizione tramite AWS Marketplace

Per poter applicare un abbonamento ad AWS Marketplace al tuo account di prova Data Infrastructure Insights esistente, devi essere un proprietario o un amministratore dell'account. Inoltre, è necessario disporre di un account Amazon Web Services (AWS).

Facendo clic sul collegamento Amazon Marketplace si apre AWS "Data Infrastructure Insights" pagina di abbonamento, dove puoi completare il tuo abbonamento. Tieni presente che i valori immessi nella calcolatrice non vengono inseriti nella pagina di sottoscrizione AWS; dovrai immettere il numero totale di unità gestite in questa pagina.

Dopo aver inserito il numero totale di unità gestite e aver scelto la durata dell'abbonamento di 12 o 36 mesi, clicca su **Configura il tuo account** per completare la procedura di abbonamento.

Una volta completato il processo di sottoscrizione ad AWS, verrai reindirizzato al tuo ambiente Data Infrastructure Insights . Oppure, se l'ambiente non è più attivo (ad esempio, se hai effettuato la

disconnessione), verrai indirizzato alla pagina di accesso della console NetAPp. Quando effettuerai nuovamente l'accesso a Data Infrastructure Insights , il tuo abbonamento sarà attivo.

> Dopo aver cliccato su **Configura il tuo account** nella pagina AWS Marketplace, devi completare la procedura di abbonamento ad AWS entro un'ora. Se non completi la procedura entro un'ora, dovrai cliccare nuovamente su **Configura il tuo account** per completarla.

Se si verifica un problema e il processo di abbonamento non viene completato correttamente, verrà comunque visualizzato il banner "Versione di prova" quando si accede al proprio ambiente. In questo caso, puoi andare su **Amministrazione > Abbonamento** e ripetere la procedura di abbonamento.

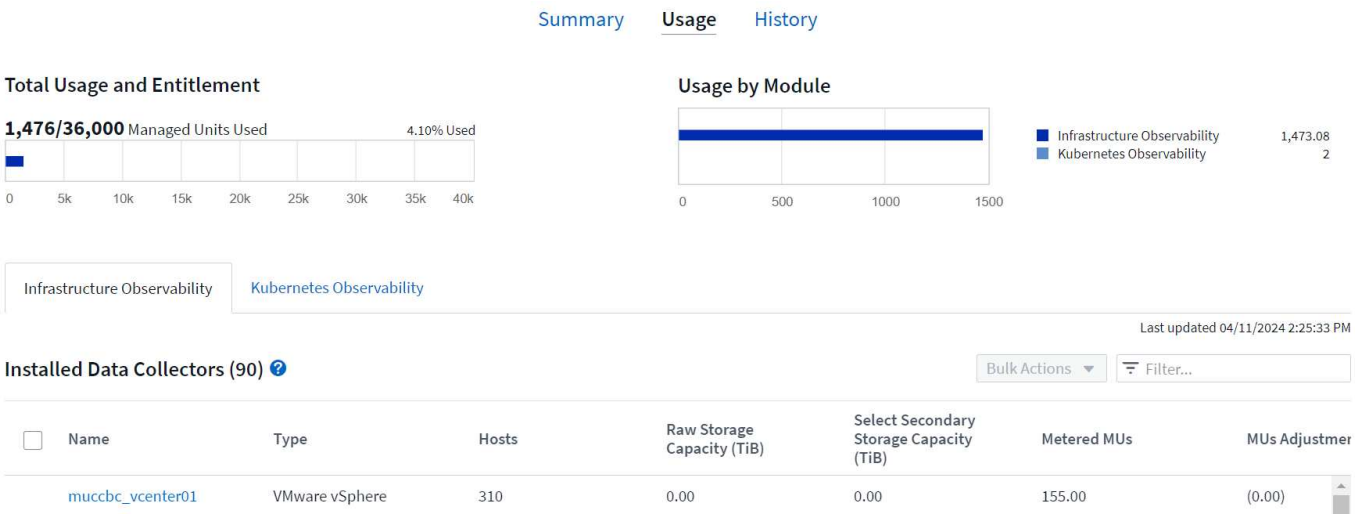
Visualizza lo stato del tuo abbonamento

Una volta attivato l'abbonamento, puoi visualizzarne lo stato e l'utilizzo delle unità gestite dalla pagina **Amministrazione > Abbonamento**.

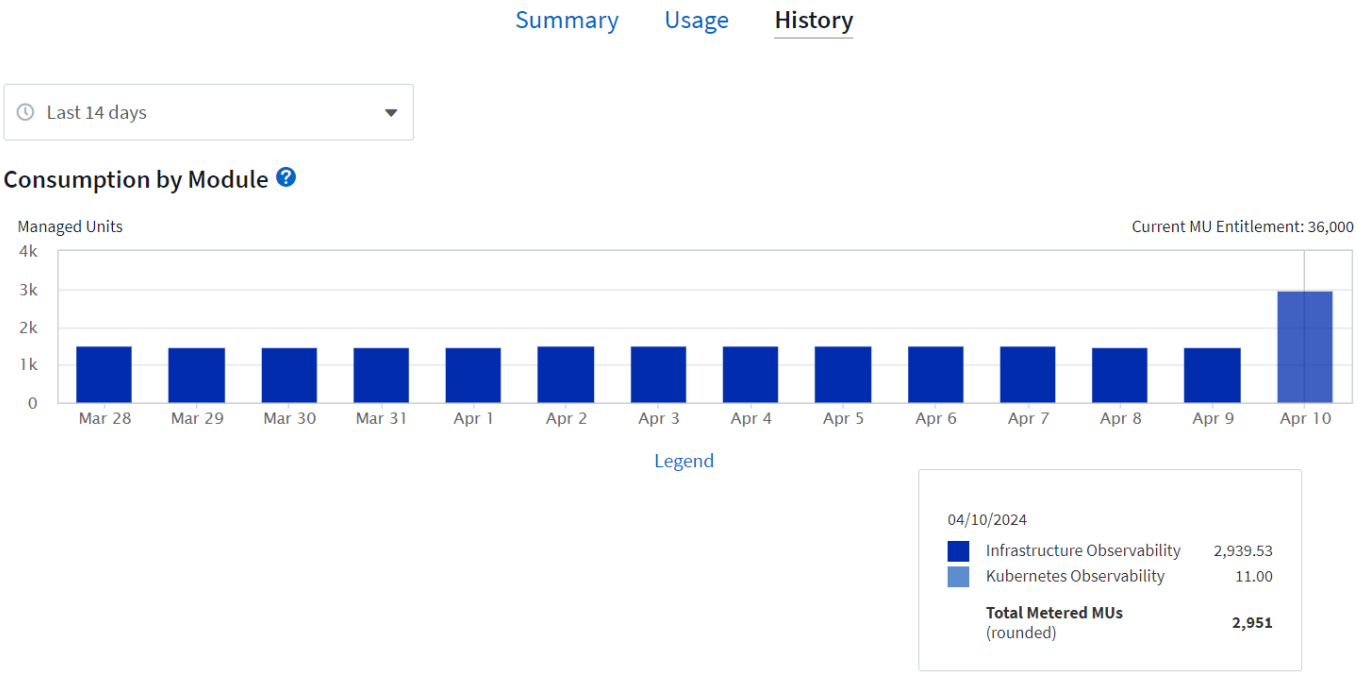
La scheda **Riepilogo** abbonamento mostra elementi come i seguenti:

- Edizione corrente
- Numero di serie dell'abbonamento
- Diritto attuale alla MU

La scheda **Utilizzo** mostra l'attuale utilizzo di MU e la suddivisione di tale utilizzo in base al raccoglitore dati.



La scheda **Cronologia** fornisce informazioni dettagliate sull'utilizzo di MU negli ultimi 7-90 giorni. Passando il mouse su una colonna del grafico si ottiene una ripartizione per modulo (ad esempio, Osservabilità, Kubernetes).



Visualizza la tua gestione dell'utilizzo

La scheda Gestione utilizzo mostra una panoramica dell'utilizzo delle unità gestite, nonché schede che suddividono il consumo delle unità gestite per collettore o cluster Kubernetes.

Il conteggio delle unità gestite con capacità non formattata riflette la somma della capacità grezza totale nell'ambiente e viene arrotondato all'unità gestita più vicina.

La somma delle unità gestite potrebbe differire leggermente dal conteggio dei raccoglitori di dati nella sezione riepilogativa. Ciò avviene perché il conteggio delle unità gestite viene arrotondato all'unità gestita più vicina. La somma di questi numeri nell'elenco dei Data Collector potrebbe essere leggermente superiore al totale delle Unità gestite nella sezione Stato. La sezione riepilogativa riflette il numero effettivo di unità gestite per il tuo abbonamento.

Nel caso in cui l'utilizzo si avvicini o superi l'importo sottoscritto, è possibile ridurlo eliminando i raccoglitori di dati o interrompendo il monitoraggio dei cluster Kubernetes. Elimina un elemento da questo elenco cliccando sul menu "tre puntini" e selezionando *Elimina*.

Cosa succede se supero l'utilizzo a cui sono iscritto?

Vengono visualizzati degli avvisi quando l'utilizzo delle unità gestite supera l'80%, il 90% e il 100% dell'importo totale sottoscritto:

Quando l'utilizzo supera:	Questo accade / Azione consigliata:
80%	Viene visualizzato un banner informativo. Non è necessaria alcuna azione.
90%	Viene visualizzato un banner di avviso. Potresti voler aumentare il numero di unità gestite a cui sei iscritto.

Quando l'utilizzo supera:	Questo accade / Azione consigliata:
100%	Un banner di errore viene visualizzato finché non si esegue una delle seguenti operazioni: • Rimuovere i Data Collector in modo che l'utilizzo delle unità gestite sia pari o inferiore all'importo sottoscritto • Modifica il tuo abbonamento per aumentare il numero di unità gestite sottoscritte

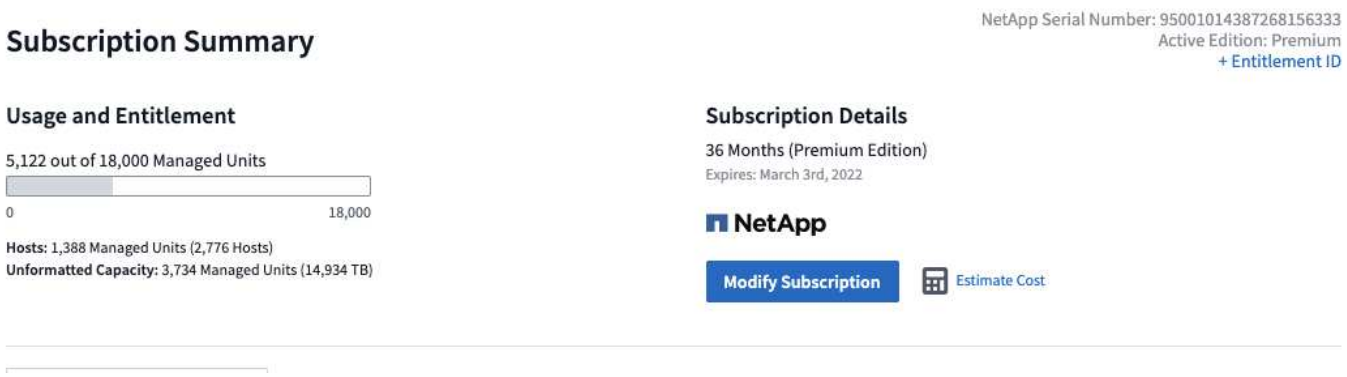
Iscriviti direttamente e salta la prova

Puoi anche iscriverti a Data Infrastructure Insights direttamente da "Mercato AWS" , senza prima creare un ambiente di prova. Una volta completata la sottoscrizione e configurato l'ambiente, l'iscrizione sarà immediata.

Aggiunta di un ID di autorizzazione

Se possiedi un prodotto NetApp valido in bundle con Data Infrastructure Insights, puoi aggiungere il numero di serie di quel prodotto al tuo abbonamento Data Infrastructure Insights esistente. Ad esempio, se hai acquistato NetApp Astra Control Center, il numero di serie della licenza Astra Control Center può essere utilizzato per identificare l'abbonamento in Data Infrastructure Insights. Data Infrastructure Insights fa riferimento a questo come *ID di autorizzazione*.

Per aggiungere un ID di autorizzazione al tuo abbonamento a Data Infrastructure Insights , nella pagina **Amministrazione > Abbonamento**, fai clic su *+ID autorizzazione*.



Osservabilità

Creazione di dashboard

Panoramica delle dashboard

Data Infrastructure Insights offre agli utenti la flessibilità di creare visualizzazioni operative dei dati dell'infrastruttura, consentendo di creare dashboard personalizzate con una varietà di widget, ognuno dei quali offre un'ampia flessibilità nella visualizzazione e nella rappresentazione grafica dei dati.

> Gli esempi riportati in queste sezioni hanno solo scopo esplicativo e non coprono tutti gli scenari possibili. I concetti e i passaggi descritti in questo documento possono essere utilizzati per creare dashboard personalizzate, evidenziando i dati specifici per le proprie esigenze specifiche.

Creazione di una dashboard

Puoi creare una nuova dashboard in uno dei due posti seguenti:

- **Dashboard > [+Nuova dashboard]**
- **Dashboard > Mostra tutte le dashboard >** clicca sul pulsante **[+Dashboard]**

Guardalo in azione

Crea dashboard potenti con NetApp (video),window=read-later

Controlli del cruscotto

La schermata Dashboard presenta diversi controlli:

- **Selettore di tempo**: consente di visualizzare i dati della dashboard per un intervallo di tempo che va dagli ultimi 15 minuti agli ultimi 30 giorni oppure per un intervallo di tempo personalizzato fino a 31 giorni. È possibile scegliere di ignorare questo intervallo di tempo globale nei singoli widget.
- Pulsante **Salva**: consente di salvare o eliminare la dashboard.

  È possibile rinominare la dashboard corrente facendo clic su **Rinomina** dal menu Salva.

- Pulsante **+ Aggiungi widget**, che consente di aggiungere un numero qualsiasi di tabelle, grafici o altri widget alla dashboard.

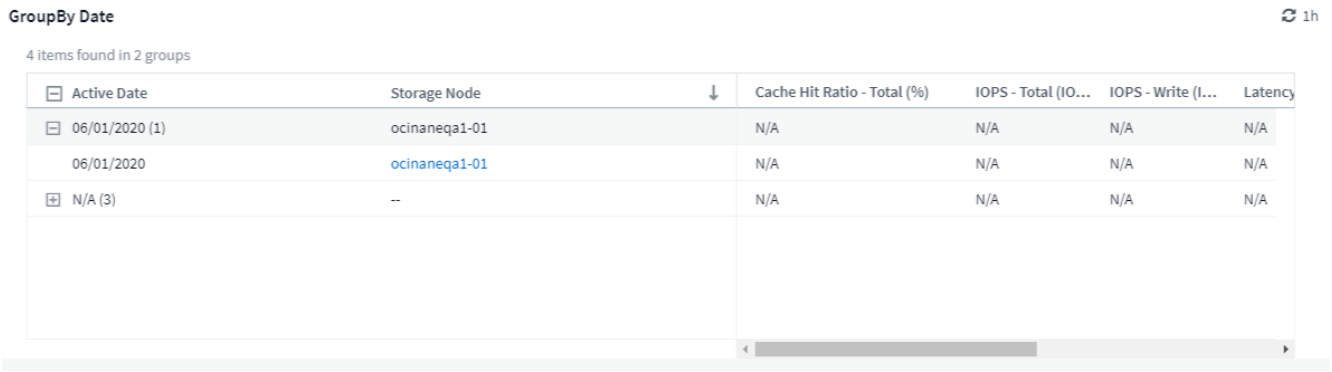
  I widget possono essere ridimensionati e riposizionati in diverse posizioni all'interno della dashboard, per offrirti la migliore visualizzazione dei tuoi dati in base alle tue esigenze attuali.

- Pulsante **+ Aggiungi variabile**, che consente di utilizzare variabili per filtrare attivamente i dati della dashboard.

Tipi di widget

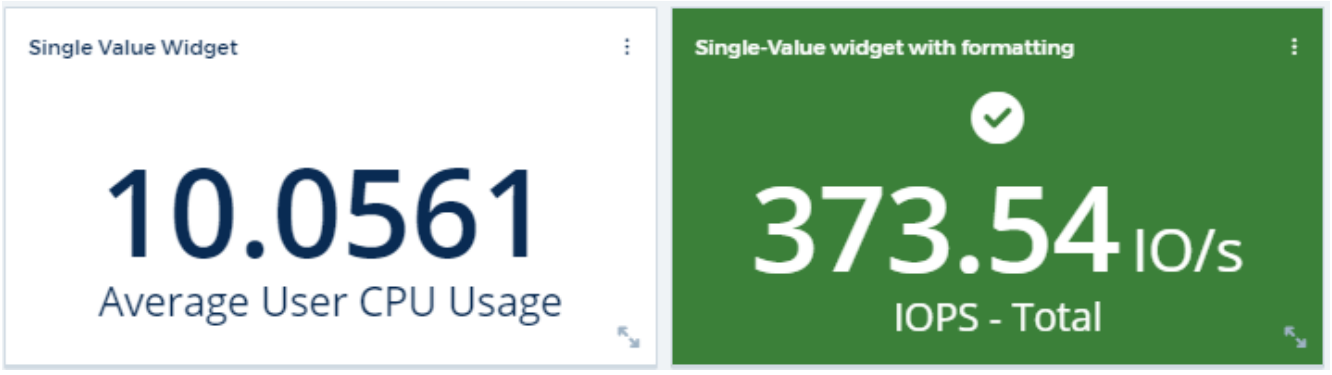
Puoi scegliere tra i seguenti tipi di widget:

- **Widget Tabella**: una tabella che visualizza i dati in base ai filtri e alle colonne scelti. I dati della tabella possono essere combinati in gruppi che possono essere compressi ed espansi.

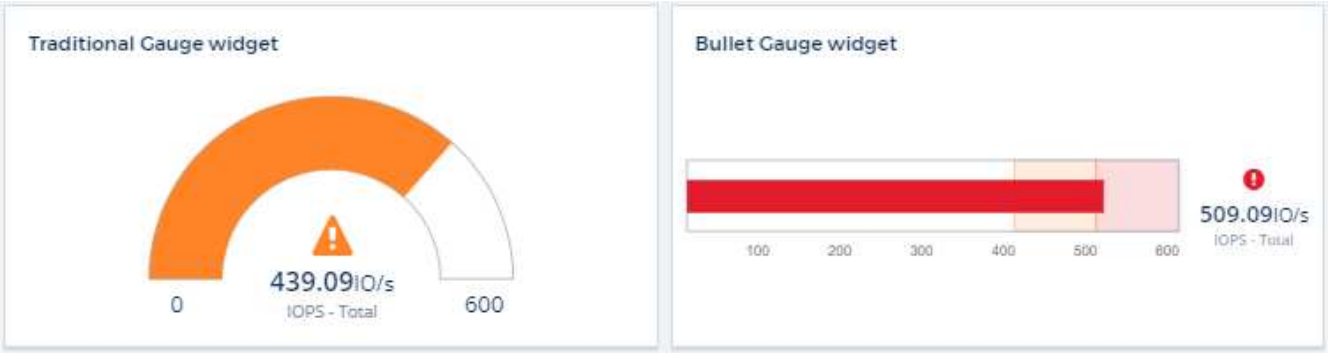


- **Grafici a linee, spline, ad area e ad area impilata**: si tratta di widget grafici di serie temporali su cui è possibile visualizzare le prestazioni e altri dati nel tempo.

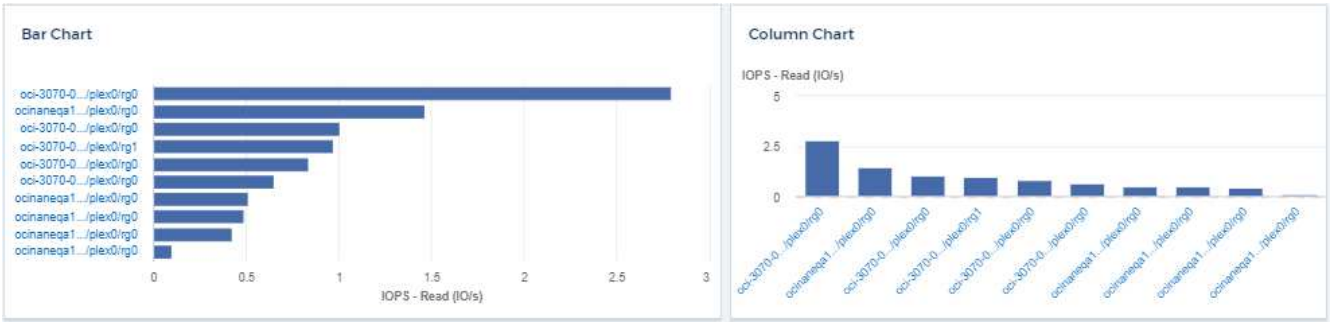
- **Widget Valore singolo**: un widget che consente di visualizzare un singolo valore che può essere derivato direttamente da un contatore o calcolato tramite una query o un'espressione. È possibile definire soglie di formattazione del colore per indicare se il valore rientra nell'intervallo previsto, di avviso o critico.



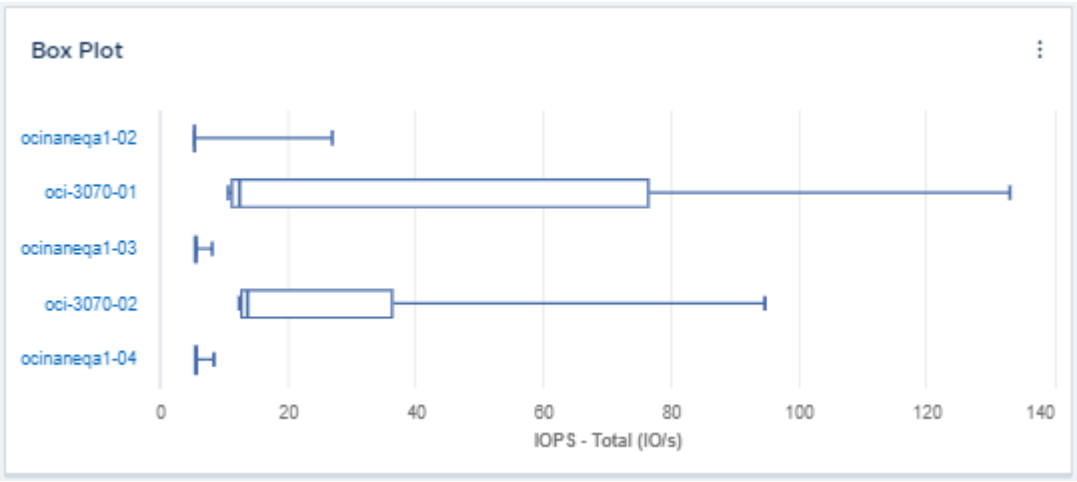
- **Widget indicatore**: visualizza i dati a valore singolo in un indicatore tradizionale (solido) o in un indicatore a proiettile, con colori basati sui valori "Avvertenza" o "Critici" che"personalizzare" .



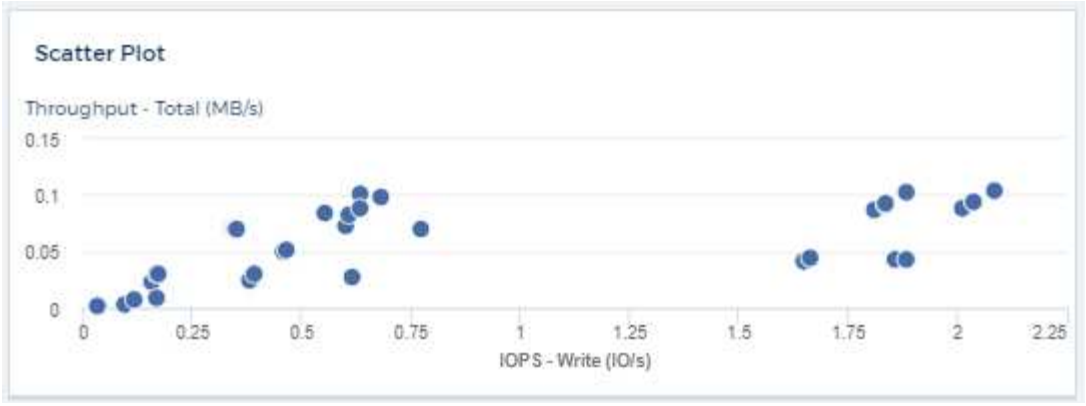
- **Grafici a barre e a colonne**: visualizza i valori N più alti o più bassi, ad esempio i primi 10 archivi in base alla capacità o gli ultimi 5 volumi in base agli IOPS.



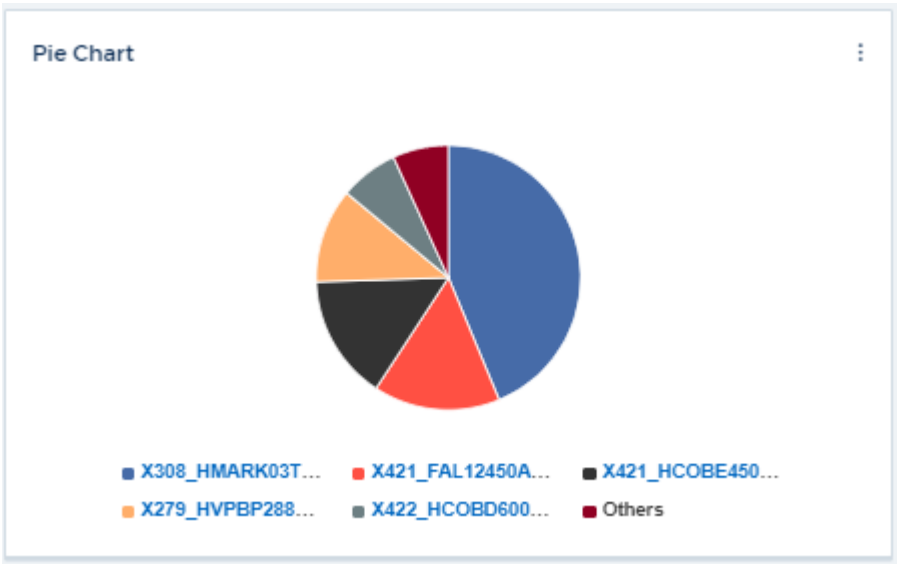
- **Grafico a scatola**: un grafico che rappresenta il minimo, il massimo, la mediana e l'intervallo tra il quartile inferiore e quello superiore dei dati in un singolo grafico.



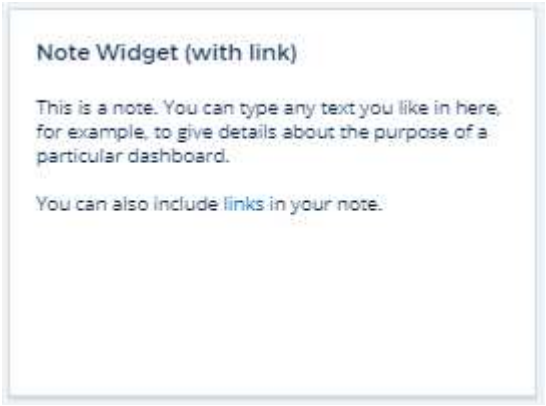
- **Grafico a dispersione**: rappresenta graficamente i dati correlati come punti, ad esempio IOPS e latenza. In questo esempio, è possibile individuare rapidamente le risorse con un throughput elevato e un basso IOPS.



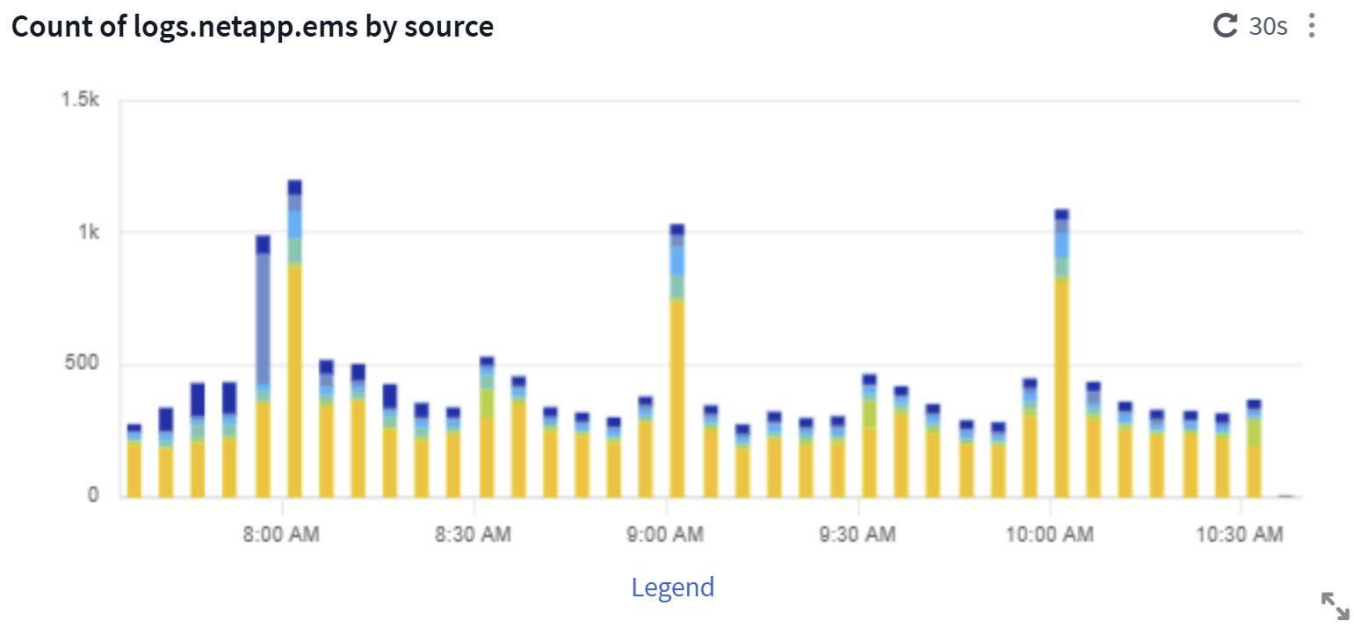
- **Grafico a torta**: un grafico a torta tradizionale per visualizzare i dati come una parte del totale.



- **Widget Nota**: fino a 1000 caratteri di testo libero.



- **Grafico a barre temporali**: visualizza i dati di registro o le metriche nel tempo.



- **Tabella avvisi**: visualizza fino agli ultimi 1.000 avvisi.

Per spiegazioni più dettagliate su queste e altre funzionalità della Dashboard,"clicca qui" .

Impostazione di una dashboard come home page

Puoi scegliere quale dashboard impostare come **home page** del tuo tenant utilizzando uno dei seguenti metodi:

- Vai a **Dashboard > Mostra tutte le dashboard** per visualizzare l'elenco delle dashboard sul tuo tenant. Fare clic sul menu delle opzioni a destra della dashboard desiderata e selezionare **Imposta come home page**.
- Fare clic su una dashboard dall'elenco per aprirla. Fare clic sul menu a discesa nell'angolo superiore e selezionare **Imposta come pagina iniziale**.

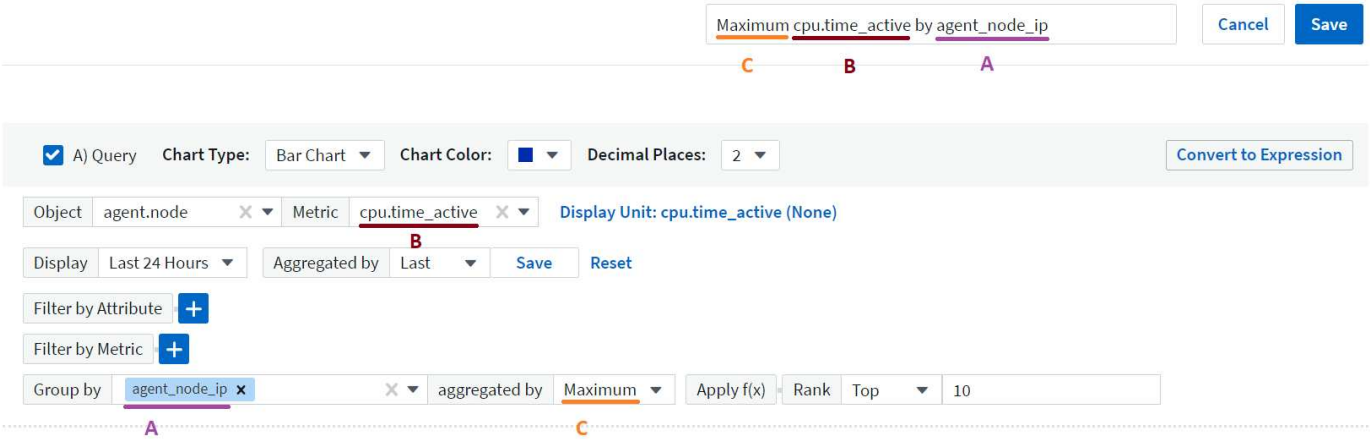
Funzionalità della dashboard

Dashboard e widget consentono una grande flessibilità nella visualizzazione dei dati. Ecco alcuni concetti che ti aiuteranno a sfruttare al meglio le tue dashboard personalizzate.

indice:[]

Denominazione dei widget

I widget vengono denominati automaticamente in base all'oggetto, alla metrica o all'attributo selezionato per la prima query del widget. Se si sceglie anche un raggruppamento per il widget, gli attributi "Raggruppa per" vengono inclusi nella denominazione automatica (metodo di aggregazione e metrica).



Selezionando un nuovo oggetto o un nuovo attributo di raggruppamento, il nome automatico viene aggiornato.

Se non si desidera utilizzare il nome automatico del widget, è sufficiente digitarne uno nuovo.

Posizionamento e dimensione del widget

Tutti i widget della dashboard possono essere posizionati e dimensionati in base alle esigenze specifiche di ogni dashboard.

Duplicazione di un widget

Nella modalità di modifica della dashboard, fare clic sul menu sul widget e selezionare **Duplica**. Viene avviato l'editor dei widget, precompilato con la configurazione del widget originale e con un suffisso "copia" nel nome del widget. Puoi apportare facilmente tutte le modifiche necessarie e salvare il nuovo widget. Il widget verrà posizionato nella parte inferiore della dashboard e potrai posizionarlo come preferisci. Ricordati di salvare la dashboard una volta completate tutte le modifiche.

Visualizzazione delle legende dei widget

La maggior parte dei widget sui dashboard può essere visualizzata con o senza legenda. Le legende nei widget possono essere attivate o disattivate su una dashboard tramite uno dei seguenti metodi:

- Quando si visualizza la dashboard, fare clic sul pulsante **Opzioni** sul widget e selezionare **Mostra legende** nel menu.

Man mano che i dati visualizzati nel widget cambiano, la legenda del widget viene aggiornata dinamicamente.

Quando vengono visualizzate le legende, se è possibile raggiungere la pagina di destinazione della risorsa indicata dalla legenda, la legenda verrà visualizzata come collegamento alla pagina di tale risorsa. Se la legenda visualizza "tutto", cliccando sul collegamento verrà visualizzata una pagina di query corrispondente alla prima query nel widget.

Trasformazione delle metriche

Data Infrastructure Insights fornisce diverse opzioni di **trasformazione** per determinate metriche nei widget (in particolare, quelle denominate "Personalizzate" o Metriche di integrazione, come quelle provenienti da Kubernetes, ONTAP Advanced Data, plugin Telegraf, ecc.), consentendo di visualizzare i dati in vari modi. Quando si aggiungono metriche trasformabili a un widget, viene visualizzato un menu a discesa che offre le seguenti opzioni di trasformazione:

Nessuno: i dati vengono visualizzati così come sono, senza alcuna manipolazione.

Tasso: valore corrente diviso per l'intervallo di tempo trascorso dall'osservazione precedente.

Cumulativo: l'accumulo della somma dei valori precedenti e del valore corrente.

Delta: la differenza tra il valore dell'osservazione precedente e il valore attuale.

Tasso delta: valore delta diviso per l'intervallo di tempo trascorso dall'osservazione precedente.

Tasso cumulativo: valore cumulativo diviso per l'intervallo di tempo trascorso dall'osservazione precedente.

Si noti che la trasformazione delle metriche non modifica i dati sottostanti in sé, ma solo il modo in cui vengono visualizzati.

Query e filtri del widget della dashboard

Query

La query in un widget della dashboard è uno strumento potente per gestire la visualizzazione dei dati. Ecco alcune cose da tenere a mente sulle query dei widget.

Alcuni widget possono avere fino a cinque query. Ogni query traccerà il proprio insieme di linee o grafici nel widget. L'impostazione di rollup, raggruppamento, risultati in alto/in basso, ecc. su una query non influisce sulle altre query per il widget.

È possibile fare clic sull'icona a forma di occhio per nascondere temporaneamente una query. La visualizzazione del widget si aggiorna automaticamente quando si nasconde o si mostra una query. Ciò consente di controllare i dati visualizzati per singole query durante la creazione del widget.

I seguenti tipi di widget possono avere più query:

- Grafico ad area
- Grafico ad area impilata
- Grafico a linee
- Grafico spline
- Widget a valore singolo

I restanti tipi di widget possono avere una sola query:

- Tavolo
- Grafico a barre
- Diagramma a scatola
- Diagramma di dispersione

Filtraggio nelle query del widget della dashboard

Ecco alcune cose che puoi fare per sfruttare al meglio i tuoi filtri.

Filtraggio della corrispondenza esatta

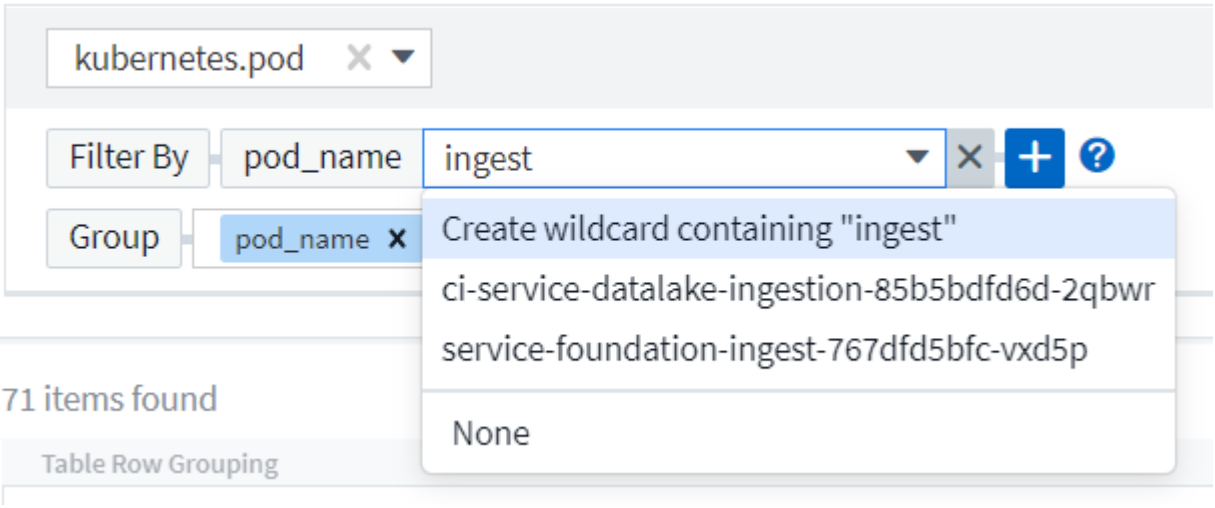
Se si racchiude una stringa di filtro tra virgolette doppie, Insight considera tutto ciò che si trova tra la prima e

l'ultima virgoletta come una corrispondenza esatta. Tutti i caratteri speciali o gli operatori all'interno delle virgolette verranno trattati come valori letterali. Ad esempio, filtrando per "*" si otterranno risultati che sono un asterisco letterale; in questo caso l'asterisco non verrà trattato come un carattere jolly. Anche gli operatori AND, OR e NOT verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

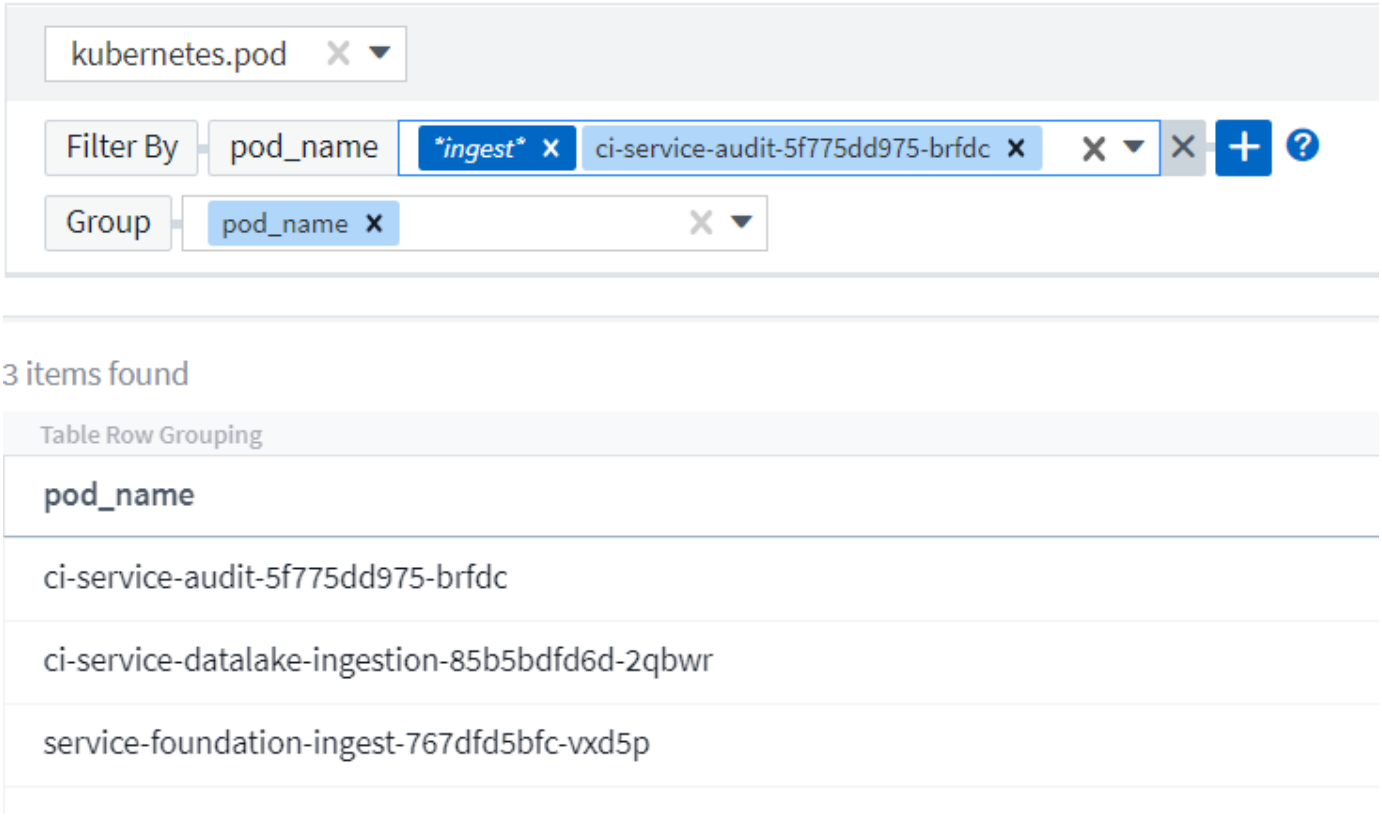
È possibile utilizzare filtri di corrispondenza esatta per trovare risorse specifiche, ad esempio il nome host. Se vuoi trovare solo il nome host 'marketing' ma escludere 'marketing01', 'marketing-boston', ecc., basta racchiudere il nome "marketing" tra virgolette doppie.

Caratteri jolly ed espressioni

Quando si filtrano valori di testo o di elenco in query o widget della dashboard, quando si inizia a digitare viene presentata l'opzione per creare un **filtro con caratteri jolly** in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione jolly. È anche possibile creare **espressioni** utilizzando NOT o OR, oppure selezionare l'opzione "Nessuno" per filtrare i valori nulli nel campo.



I filtri basati su caratteri jolly o espressioni (ad esempio NOT, OR, "Nessuno", ecc.) vengono visualizzati in blu scuro nel campo filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in azzurro.



Si noti che il filtro con caratteri jolly ed espressioni funziona con testo o elenchi, ma non con valori numerici, date o valori booleani.

Filtraggio avanzato del testo con suggerimenti contestuali di completamento automatico

Il filtraggio nelle query dei widget è *contestuale*; quando selezioni uno o più valori di filtro per un campo, gli altri filtri per quella query mostreranno i valori pertinenti a quel filtro. Ad esempio, quando si imposta un filtro per un oggetto specifico *Nome*, il campo da filtrare per *Modello* mostrerà solo i valori rilevanti per quell'oggetto Nome.

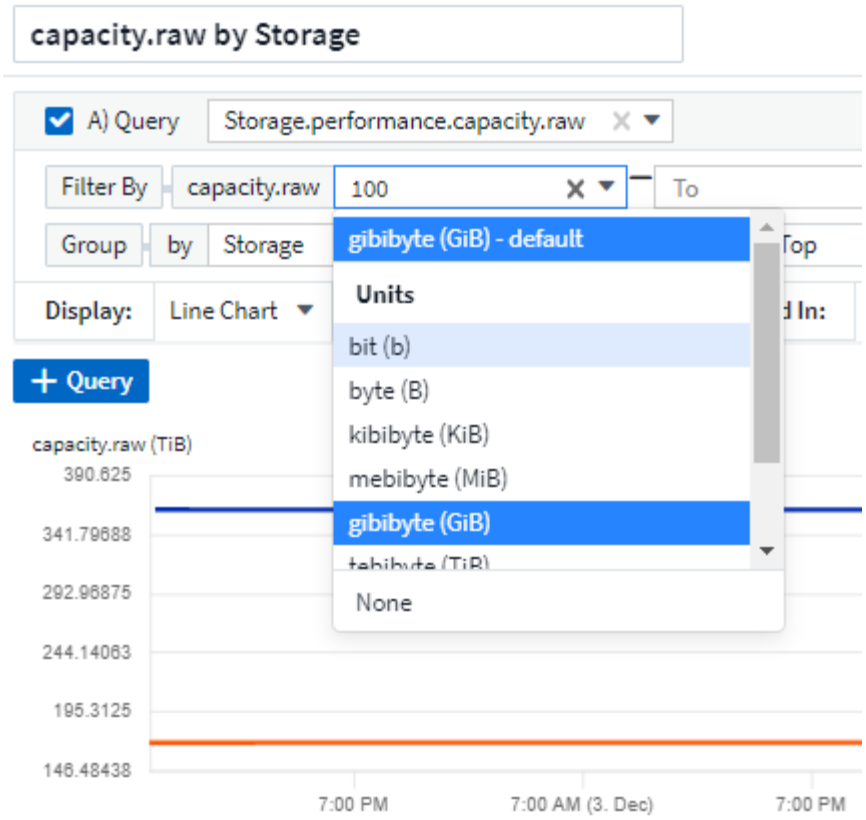
Il filtraggio contestuale si applica anche alle variabili della pagina della dashboard (solo attributi di tipo testo o annotazioni). Quando si seleziona un valore di filtro per una variabile, tutte le altre variabili che utilizzano oggetti correlati mostreranno solo i possibili valori di filtro in base al contesto di tali variabili correlate.

Tieni presente che solo i filtri di testo mostreranno suggerimenti contestuali di digitazione anticipata. Data, Enum (elenco), ecc. non mostreranno suggerimenti di completamento automatico. Detto questo, è possibile impostare un filtro su un campo Enum (ad esempio un elenco) e filtrare altri campi di testo in base al contesto. Ad esempio, selezionando un valore in un campo Enum come Data Center, altri filtri mostreranno solo i modelli/nomi in quel data center, ma non viceversa.

L'intervallo di tempo selezionato fornirà anche il contesto per i dati mostrati nei filtri.

Scelta delle unità filtranti

Mentre digiti un valore in un campo filtro, puoi selezionare le unità in cui visualizzare i valori nel grafico. Ad esempio, è possibile filtrare in base alla capacità grezza e scegliere di visualizzare il formato predefinito GiB oppure selezionare un altro formato, ad esempio TiB. Questa funzione è utile se sulla dashboard sono presenti diversi grafici che mostrano valori in TiB e si desidera che tutti i grafici mostrino valori coerenti.



Ulteriori perfezionamenti del filtraggio

Per perfezionare ulteriormente i filtri è possibile utilizzare quanto segue.

- Un asterisco consente di cercare tutto. Per esempio,

  ```
  vol*rhel
  ```

  visualizza tutte le risorse che iniziano con "vol" e finiscono con "rhel".

- Il punto interrogativo consente di cercare un numero specifico di caratteri. Per esempio,

  ```
  BOS-PRD??-S12
  ```

  visualizza *BOS-PRD12-S12*, *BOS-PRD13-S12* e così via.

- L'operatore OR consente di specificare più entità. Per esempio,

  ```
  FAS2240 OR CX600 OR FAS3270
  ```

  trova più modelli di archiviazione.

- L'operatore NOT consente di escludere del testo dai risultati della ricerca. Per esempio,

```
NOT EMC*
```

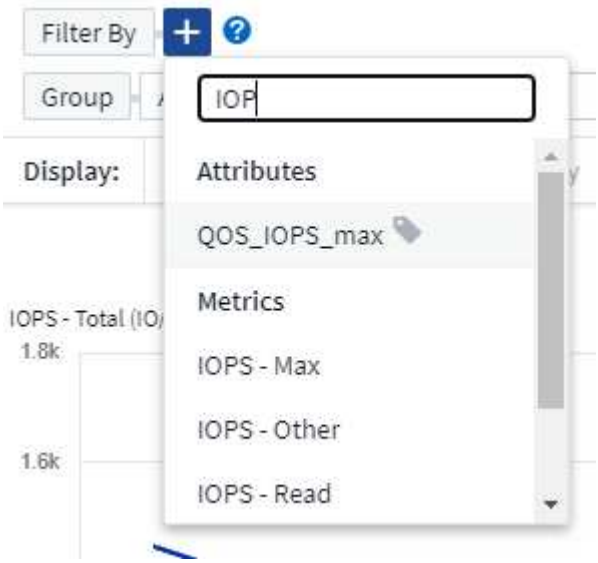
trova tutto ciò che non inizia con "EMC". Puoi usare

```
NOT *
```

per visualizzare i campi che non contengono alcun valore.

Identificazione degli oggetti restituiti da query e filtri

Gli oggetti restituiti dalle query e dai filtri sono simili a quelli mostrati nella seguente illustrazione. Gli oggetti a cui sono assegnati dei "tag" sono annotazioni, mentre gli oggetti senza tag sono contatori delle prestazioni o attributi degli oggetti.



Raggruppamento, identificazione e aggregazione

Raggruppamento (arrotolamento)

I dati visualizzati in un widget vengono raggruppati (talvolta chiamati "roll-up") a partire dai punti dati sottostanti raccolti durante l'acquisizione. Ad esempio, se si dispone di un widget grafico a linee che mostra gli IOPS di archiviazione nel tempo, potrebbe essere opportuno visualizzare una linea separata per ciascuno dei data center, per un confronto rapido. Nel campo "Raggruppa per", seleziona il tipo di oggetto stesso per visualizzare singole linee, aree, barre, colonne, ecc. (a seconda del tipo di widget) per ciascun oggetto. È possibile scegliere di raggruppare in base a qualsiasi attributo disponibile nell'elenco per quell'oggetto. Ad esempio, quando si visualizzano i dati per un volume interno, potrebbe essere opportuno raggruppare i dati in base al nome dell'archiviazione.

Per visualizzare i dati consolidati, rimuovere qualsiasi attributo Raggruppa per, che per impostazione predefinita verrà impostato sul raggruppamento per "Tutti".

Puoi scegliere di aggregare questi dati in uno dei seguenti modi:

- **Media**: visualizza ogni riga come *media* dei dati sottostanti.

- **Massimo**: visualizza ogni riga come *massimo* dei dati sottostanti.
- **Minimo**: visualizza ogni riga come *minimo* dei dati sottostanti.
- **Somma**: visualizza ogni riga come *somma* dei dati sottostanti.

Quando si visualizza la dashboard, selezionando la legenda per qualsiasi widget i cui dati sono raggruppati per "Tutti" si apre una pagina di query che mostra i risultati della prima query utilizzata nel widget.

Se hai impostato un filtro per la query, i dati vengono raggruppati in base ai dati filtrati.

Identificazione dei dati personalizzati

Quando si crea o si modifica un widget basato sui propri dati personalizzati, è possibile che i dati non vengano rappresentati correttamente nel widget senza un attributo identificativo. Se DII non riesce a identificare l'oggetto selezionato per il widget, visualizzerà un collegamento *Configurazione avanzata* nell'area "Raggruppa per". Espandi questa sezione per selezionare l'attributo con cui desideri identificare i tuoi dati.

Aggregazione dei dati

È possibile allineare ulteriormente i grafici aggregando i punti dati in intervalli di minuti, ore o giorni prima che i dati vengano successivamente raggruppati per attributo (se selezionato). È possibile scegliere di aggregare i punti dati in base alla loro *Media*, Massimo, Minimo, Somma_ o *Conteggio*.

Un intervallo piccolo combinato con un intervallo di tempo lungo potrebbe generare un avviso del tipo "L'intervallo di aggregazione ha prodotto troppi punti dati". Potresti riscontrare questo problema se hai un intervallo breve e aumenti l'intervallo di tempo della dashboard a 7 giorni. In questo caso, Insight aumenterà temporaneamente l'intervallo di aggregazione finché non si seleziona un intervallo di tempo più breve.

Per impostazione predefinita, la maggior parte dei contatori di risorse aggregano in *Media*. Per impostazione predefinita, alcuni contatori vengono aggregati in *Max, Min* o *Sum*. Ad esempio, per impostazione predefinita, gli errori delle porte vengono aggregati in *Somma*, mentre gli IOPS di archiviazione vengono aggregati in *Media*.

Visualizzazione dei risultati migliori/migliori

In un widget grafico, è possibile visualizzare i risultati **In alto** o **In basso** per i dati raggruppati e scegliere il numero di risultati visualizzati dall'elenco a discesa fornito. In un widget tabella è possibile ordinare in base a qualsiasi colonna.

Widget grafico in alto/in basso

In un widget grafico, quando si sceglie di raggruppare i dati in base a un attributo specifico, è possibile visualizzare i primi N risultati o gli ultimi N risultati. Tieni presente che non puoi scegliere i risultati migliori o peggiori quando scegli di raggruppare per *tutti* gli attributi.

È possibile scegliere quali risultati visualizzare selezionando **In alto** o **In basso** nel campo **Mostra** della query e selezionando un valore dall'elenco fornito.

Il widget della tabella mostra le voci

In un widget tabella, puoi selezionare il numero di risultati visualizzati nei risultati della tabella. Non ti viene data la possibilità di scegliere i risultati migliori o peggiori perché la tabella ti consente di ordinare in ordine crescente o decrescente in base a qualsiasi colonna a richiesta.

È possibile scegliere il numero di risultati da visualizzare nella tabella sulla dashboard selezionando un valore dal campo **Mostra voci** della query.

Widget di raggruppamento nella tabella

I dati in un widget tabella possono essere raggruppati in base a qualsiasi attributo disponibile, consentendo di visualizzare una panoramica dei dati e di approfondirli per ottenere maggiori dettagli. Le metriche nella tabella sono raggruppate in modo da facilitarne la visualizzazione in ogni riga compressa.

I widget tabella consentono di raggruppare i dati in base agli attributi impostati. Ad esempio, potresti voler visualizzare nella tabella gli IOPS totali di storage raggruppati in base ai data center in cui risiedono tali storage. Oppure potresti voler visualizzare una tabella delle macchine virtuali raggruppate in base all'hypervisor che le ospita. Dall'elenco è possibile espandere ciascun gruppo per visualizzare le risorse in esso contenute.

Il raggruppamento è disponibile solo nel tipo di widget Tabella.

Esempio di raggruppamento (con spiegazione del rollup)

I widget tabella consentono di raggruppare i dati per una visualizzazione più semplice.

In questo esempio creeremo un widget tabella che mostra tutte le VM raggruppate per Data Center.

Passi

1. Crea o apri una dashboard e aggiungi un widget **Tabella**.
2. Seleziona *Macchina virtuale* come tipo di risorsa per questo widget.
3. Fare clic sul Selettore di colonna e scegliere *Nome hypervisor* e *IOPS - Totale*.

   Tali colonne vengono ora visualizzate nella tabella.

4. Ignoriamo le VM senza IOPS e includiamo solo le VM con un IOPS totale maggiore di 1. Fare clic sul pulsante **Filtra per [+]** e selezionare *IOPS - Totale*. Fare clic su *Qualsiasi* e nel campo **da** digitare **1**. Lasciare vuoto il campo **a**. Premi Invio o fai clic fuori dal campo filtro per applicare il filtro.

   Nella tabella vengono ora visualizzate tutte le VM con IOPS totali maggiori o uguali a 1. Si noti che nella tabella non è presente alcun raggruppamento. Vengono visualizzate tutte le VM.

5. Fare clic sul pulsante **Raggruppa per [+]**.

   È possibile raggruppare in base a qualsiasi attributo o annotazione mostrata. Selezionare *Tutti* per

visualizzare tutte le VM in un unico gruppo.

Ogni intestazione di colonna per una metrica delle prestazioni visualizza un menu a "tre punti" contenente un'opzione **Roll-up**. Il metodo di rollup predefinito è *Media*. Ciò significa che il numero mostrato per il gruppo è la media di tutti gli IOPS totali segnalati per ogni VM all'interno del gruppo. È possibile scegliere di suddividere questa colonna in base a *Media, Somma, Minimo* o *Massimo*. Ogni colonna visualizzata che contiene metriche sulle prestazioni può essere raggruppata singolarmente.

6. Fare clic su *Tutti* e selezionare *Nome hypervisor*.

   L'elenco delle VM è ora raggruppato per Hypervisor. È possibile espandere ciascun hypervisor per visualizzare le VM ospitate.

7. Fare clic su **Salva** per salvare la tabella nella dashboard. È possibile ridimensionare o spostare il widget a piacere.
8. Fare clic su **Salva** per salvare la dashboard.

Riepilogo dei dati sulle prestazioni

Se si include una colonna per i dati sulle prestazioni (ad esempio, *IOPS - Totale*) in un widget tabella, quando si sceglie di raggruppare i dati è possibile scegliere un metodo di rollup per quella colonna. Il metodo di rollup predefinito consiste nel visualizzare la media (*avg*) dei dati sottostanti nella riga del gruppo. È anche possibile scegliere di visualizzare la somma, il minimo o il massimo dei dati.

Selettore intervallo di tempo della dashboard

Puoi selezionare l'intervallo di tempo per i dati della dashboard. Nei widget della dashboard verranno visualizzati solo i dati rilevanti per l'intervallo di tempo selezionato. È possibile selezionare tra i seguenti intervalli di tempo:

- Ultimi 15 minuti
- Ultimi 30 minuti
- Ultimi 60 minuti
- Ultime 2 ore

- Ultime 3 ore (questo è il valore predefinito)
- Ultime 6 ore
- Ultime 12 ore
- Ultime 24 ore
- Ultimi 2 giorni
- Ultimi 3 giorni
- Ultimi 7 giorni
- Ultimi 30 giorni
- Intervallo di tempo personalizzato

  L'intervallo di tempo personalizzato consente di selezionare fino a 31 giorni consecutivi. È anche possibile impostare l'ora di inizio e l'ora di fine del giorno per questo intervallo. L'ora di inizio predefinita è 00:00 del primo giorno selezionato e l'ora di fine predefinita è 23:59 dell'ultimo giorno selezionato. Facendo clic su **Applica** l'intervallo di tempo personalizzato verrà applicato alla dashboard.

Zoom su un intervallo di tempo

Durante la visualizzazione di un widget di serie temporali (linea, spline, area, area sovrapposta) o di un grafico su una landing page, è possibile trascinare il mouse sul grafico per ingrandire. Nell'angolo in alto a destra dello schermo è quindi possibile bloccare l'intervallo di tempo in modo che i grafici su altre pagine riflettano i dati per quell'intervallo di tempo bloccato. Per sbloccare, seleziona un intervallo di tempo diverso dall'elenco.

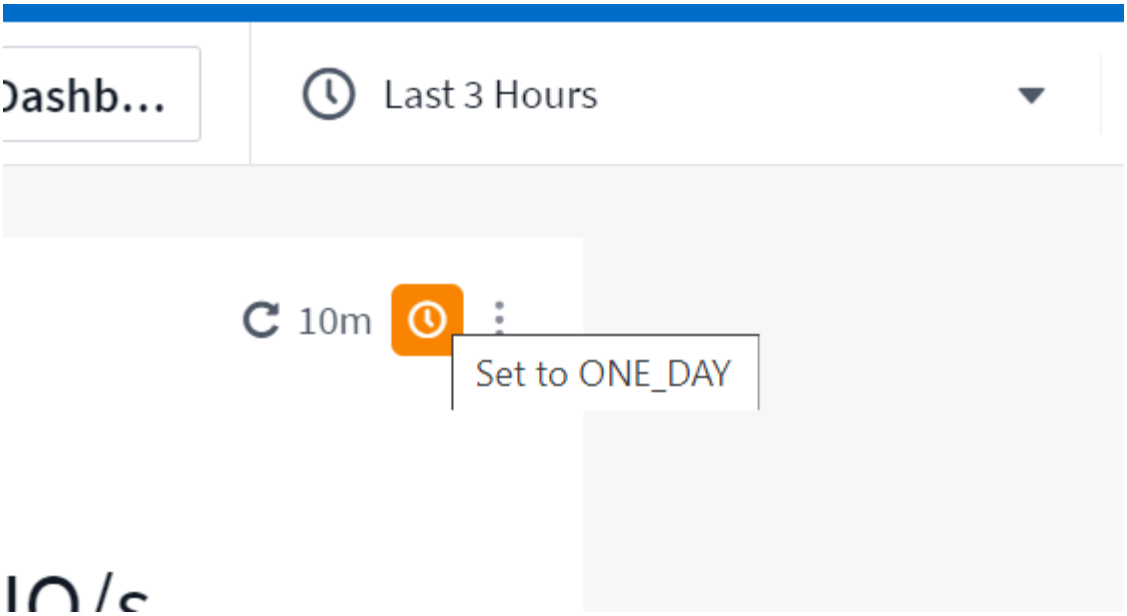
Sovrascrivere il tempo della dashboard nei singoli widget

È possibile ignorare l'impostazione dell'intervallo di tempo della dashboard principale nei singoli widget. Questi widget visualizzeranno i dati in base all'intervallo di tempo impostato, non all'intervallo di tempo della dashboard.

Per ignorare l'orario della dashboard e forzare un widget a utilizzare il proprio intervallo di tempo, nella modalità di modifica del widget, scegliere l'intervallo di tempo desiderato e salvare il widget nella dashboard.

Il widget visualizzerà i suoi dati in base all'intervallo di tempo impostato, indipendentemente dall'intervallo di tempo selezionato sulla dashboard stessa.

L'intervallo di tempo impostato per un widget non influirà sugli altri widget presenti nella dashboard.



Asse primario e secondario

Metriche diverse utilizzano unità di misura diverse per i dati riportati in un grafico. Ad esempio, quando si considerano gli IOPS, l'unità di misura è il numero di operazioni I/O al secondo (IO/s), mentre la latenza è puramente una misura del tempo (millisecondi, microsecondi, secondi, ecc.). Quando si rappresentano entrambe le metriche su un grafico a linea singola utilizzando un singolo set di valori per l'asse Y, i numeri di latenza (in genere una manciata di millisecondi) vengono rappresentati sulla stessa scala degli IOPS (in genere espressi in migliaia) e la linea di latenza si perde in quella scala.

Ma è possibile rappresentare entrambi i set di dati in un unico grafico significativo, impostando un'unità di misura sull'asse Y primario (lato sinistro) e l'altra unità di misura sull'asse Y secondario (lato destro). Ogni metrica è rappresentata graficamente secondo una scala propria.

Passi

Questo esempio illustra il concetto di assi primari e secondari in un widget grafico.

1. Crea o apri una dashboard. Aggiungi un widget grafico a linee, grafico spline, grafico ad area o grafico ad area impilata alla dashboard.
2. Seleziona un tipo di risorsa (ad esempio *Archiviazione*) e scegli *IOPS - Totale* come prima metrica. Imposta i filtri che preferisci e, se lo desideri, scegli un metodo di aggregazione.

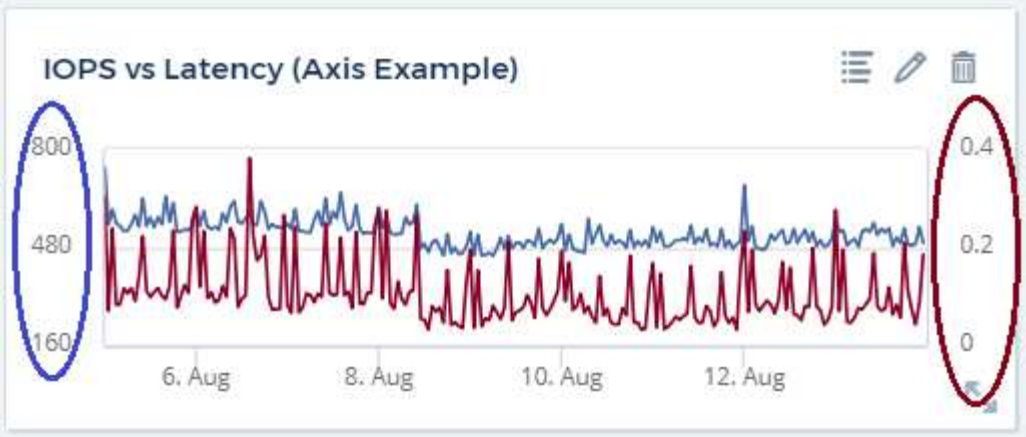
   La linea IOPS viene visualizzata sul grafico, con la sua scala indicata sulla sinistra.

3. Fare clic su **[+Query]** per aggiungere una seconda riga al grafico. Per questa riga, seleziona *Latenza - Totale* come metrica.

   Si noti che la linea viene visualizzata piatta nella parte inferiore del grafico. Ciò avviene perché viene disegnato *alla stessa scala* della linea IOPS.

4. Nella query Latenza, seleziona **Asse Y: Secondario**.

   La linea della latenza è ora disegnata con una scala propria, visualizzata sul lato destro del grafico.



Espressioni nei widget

In una dashboard, qualsiasi widget di serie temporali (linee, spline, aree, aree impilate), grafico a barre, istogramma, grafico a torta o widget di tabella consente di creare espressioni dalle metriche scelte e di mostrare il risultato di tali espressioni in un singolo grafico (o colonna nel caso diwidget di tabella). Gli esempi seguenti utilizzano espressioni per risolvere problemi specifici. Nel primo esempio, vogliamo mostrare gli IOPS di lettura come percentuale degli IOPS totali per tutte le risorse di archiviazione nel tenant. Il secondo esempio fornisce visibilità sugli IOPS di "sistema" o "overhead" che si verificano sul tenant, ovvero quegli IOPS che non derivano direttamente dalla lettura o dalla scrittura dei dati.

È possibile utilizzare variabili nelle espressioni (ad esempio, *$Var1 * 100*)

Esempio di espressioni: Leggi la percentuale IOPS

In questo esempio, vogliamo mostrare gli IOPS di lettura come percentuale degli IOPS totali. Si può pensare a questo come alla seguente formula:

```
 Read Percentage = (Read IOPS / Total IOPS) x 100
Questi dati possono essere visualizzati in un grafico a linee sulla
dashboard.  Per fare ciò, segui questi passaggi:
```

Passi

1. Crea una nuova dashboard oppure aprine una esistente in modalità di modifica.
2. Aggiungi un widget alla dashboard. Seleziona **Grafico ad area**.

   Il widget si apre in modalità di modifica. Per impostazione predefinita, viene visualizzata una query che mostra *IOPS - Totale* per le risorse di *archiviazione*. Se lo desideri, seleziona un tipo di risorsa diverso.

3. Fare clic sul collegamento **Converti in espressione** a destra.

   La query corrente viene convertita in modalità Espressione. Tieni presente che non è possibile modificare il tipo di risorsa mentre sei in modalità Espressione. Mentre sei in modalità Espressione, il collegamento cambia in **Ripristina query**. Fare clic qui se si desidera tornare in qualsiasi momento alla modalità Query. Tieni presente che il passaggio da una modalità all'altra ripristinerà i campi ai valori predefiniti.

   Per ora, mantieni la modalità Espressione.

4. La metrica **IOPS - Totale** si trova ora nel campo variabile alfabetico "**a**". Nel campo variabile "**b**", fare clic

su **Seleziona** e scegliere **IOPS - Lettura**.

È possibile aggiungere fino a un totale di cinque variabili alfabetiche per l'espressione facendo clic sul pulsante + dopo i campi delle variabili. Per il nostro esempio di percentuale di lettura, abbiamo bisogno solo di IOPS totali ("**a**") e IOPS di lettura ("**b**").

5. Nel campo **Espressione**, utilizzare le lettere corrispondenti a ciascuna variabile per creare l'espressione. Sappiamo che la percentuale di lettura è = (IOPS di lettura / IOPS totali) x 100, quindi scriveremmo questa espressione come:

```
 (b / a) * 100
. Il campo *Etichetta* identifica l'espressione.  Cambia l'etichetta in
"Percentuale di lettura" o in qualcosa di altrettanto significativo per
te.
. Modificare il campo *Unità* in "%" o "Percentuale".
```

Il grafico mostra la percentuale di lettura IOPS nel tempo per i dispositivi di archiviazione scelti. Se lo desideri, puoi impostare un filtro o scegliere un metodo di rollup diverso. Tieni presente che se selezioni Somma come metodo di aggregazione, tutti i valori percentuali vengono sommati e potrebbero potenzialmente superare il 100%.

6. Fare clic su **Salva** per salvare il grafico nella dashboard.

Esempio di espressioni: I/O "Sistema"

Esempio 2: Tra le metriche raccolte dalle fonti dati ci sono lettura, scrittura e IOPS totali. Tuttavia, il numero totale di IOPS riportato da una fonte dati a volte include gli IOPS "di sistema", ovvero quelle operazioni di I/O che non fanno parte direttamente della lettura o della scrittura dei dati. Questo I/O di sistema può anche essere considerato un I/O "overhead", necessario per il corretto funzionamento del sistema ma non direttamente correlato alle operazioni sui dati.

Per visualizzare questi I/O di sistema, è possibile sottrarre gli IOPS di lettura e scrittura dagli IOPS totali riportati dall'acquisizione. La formula potrebbe essere la seguente:

```
 System IOPS = Total IOPS - (Read IOPS + Write IOPS)
Questi dati possono quindi essere visualizzati in un grafico a linee sulla
dashboard.  Per fare ciò, segui questi passaggi:
```

Passi

1. Crea una nuova dashboard oppure aprine una esistente in modalità di modifica.
2. Aggiungi un widget alla dashboard. Seleziona **Grafico a linee**.

   Il widget si apre in modalità di modifica. Per impostazione predefinita, viene visualizzata una query che mostra *IOPS - Totale* per le risorse di *archiviazione*. Se lo desideri, seleziona un tipo di risorsa diverso.

3. Nel campo **Arrotonda**, seleziona *Somma* per *Tutti*.

   Il grafico mostra una linea che mostra la somma degli IOPS totali.

4. Fare clic sull'icona *Duplica questa query* per creare una copia della query.

Un duplicato della query viene aggiunto sotto l'originale.

5. Nella seconda query, fare clic sul pulsante **Converti in espressione**.

   La query corrente viene convertita in modalità Espressione. Fare clic su **Ripristina query** se si desidera tornare alla modalità query in qualsiasi momento. Tieni presente che il passaggio da una modalità all'altra ripristinerà i campi ai valori predefiniti.

   Per ora, mantieni la modalità Espressione.

6. La metrica *IOPS - Totale* si trova ora nel campo variabile alfabetico "**a**". Fare clic su *IOPS - Totale* e modificarlo in *IOPS - Lettura*.
7. Nel campo variabile "**b**", fare clic su **Seleziona** e scegliere *IOPS - Scrivi*.
8. Nel campo **Espressione**, utilizzare le lettere corrispondenti a ciascuna variabile per creare l'espressione. Scriveremmo la nostra espressione semplicemente come:

   ```
   a + b
   ```

   Nella sezione Visualizzazione, seleziona **Grafico ad area** per questa espressione.

9. Il campo **Etichetta** identifica l'espressione. Cambia l'etichetta in "IOPS di sistema" o in qualcosa di altrettanto significativo per te.

   Il grafico mostra gli IOPS totali come un grafico a linee, con un grafico ad area che mostra la combinazione di IOPS in lettura e scrittura al di sotto. Il divario tra i due mostra gli IOPS che non sono direttamente correlati alle operazioni di lettura o scrittura dei dati. Questi sono gli IOPS del "sistema".

10. Fare clic su **Salva** per salvare il grafico nella dashboard.

Per utilizzare una variabile in un'espressione, è sufficiente digitare il nome della variabile, ad esempio *$var1 * 100*. Nelle espressioni è possibile utilizzare solo variabili numeriche.

Espressioni in un widget tabella

I widget tabella gestiscono le espressioni in modo leggermente diverso. È possibile avere fino a cinque espressioni in un singolo widget tabella, ciascuna delle quali viene aggiunta come nuova colonna alla tabella. Ogni espressione può includere fino a cinque valori su cui eseguire il calcolo. Puoi facilmente dare alla colonna un nome significativo.

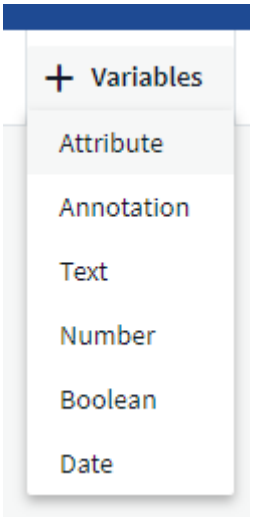
Variabili

Le variabili consentono di modificare contemporaneamente i dati visualizzati in alcuni o in tutti i widget di una dashboard. Impostando uno o più widget in modo che utilizzino una variabile comune, le modifiche apportate in un punto determinano l'aggiornamento automatico dei dati visualizzati in ciascun widget.

Tipi di variabili

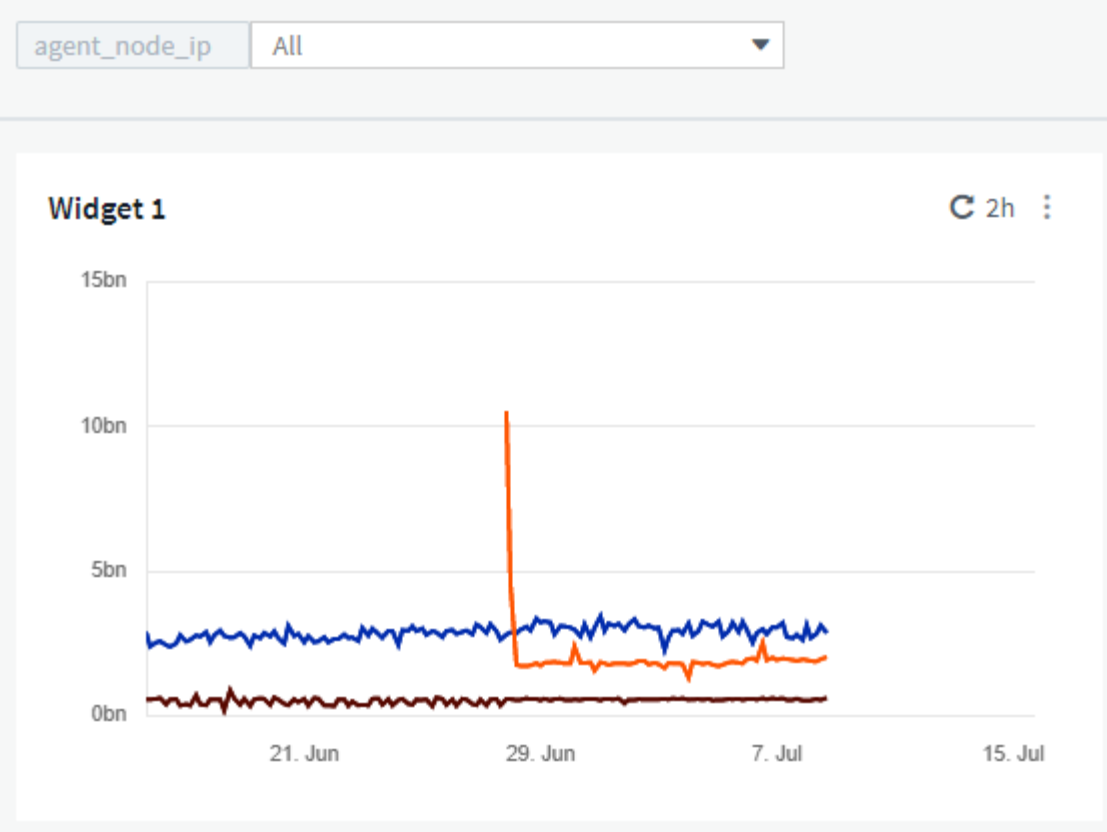
Una variabile può essere di uno dei seguenti tipi:

- **Attributo**: utilizza gli attributi o le metriche di un oggetto per filtrare
- **Annotazione**: Utilizzare un predefinito"Annotazione" per filtrare i dati del widget.
- **Testo**: Una stringa alfanumerica.
- **Numerico**: un valore numerico. Utilizzabile da solo o come valore "da" o "a", a seconda del campo del widget.
- **Booleano**: utilizzare per i campi con valori Vero/Falso, Sì/No, ecc. Per la variabile booleana, le scelte sono Sì, No, Nessuno, Qualsiasi.
- **Data**: un valore di data. Utilizzare come valore "da" o "a", a seconda della configurazione del widget.

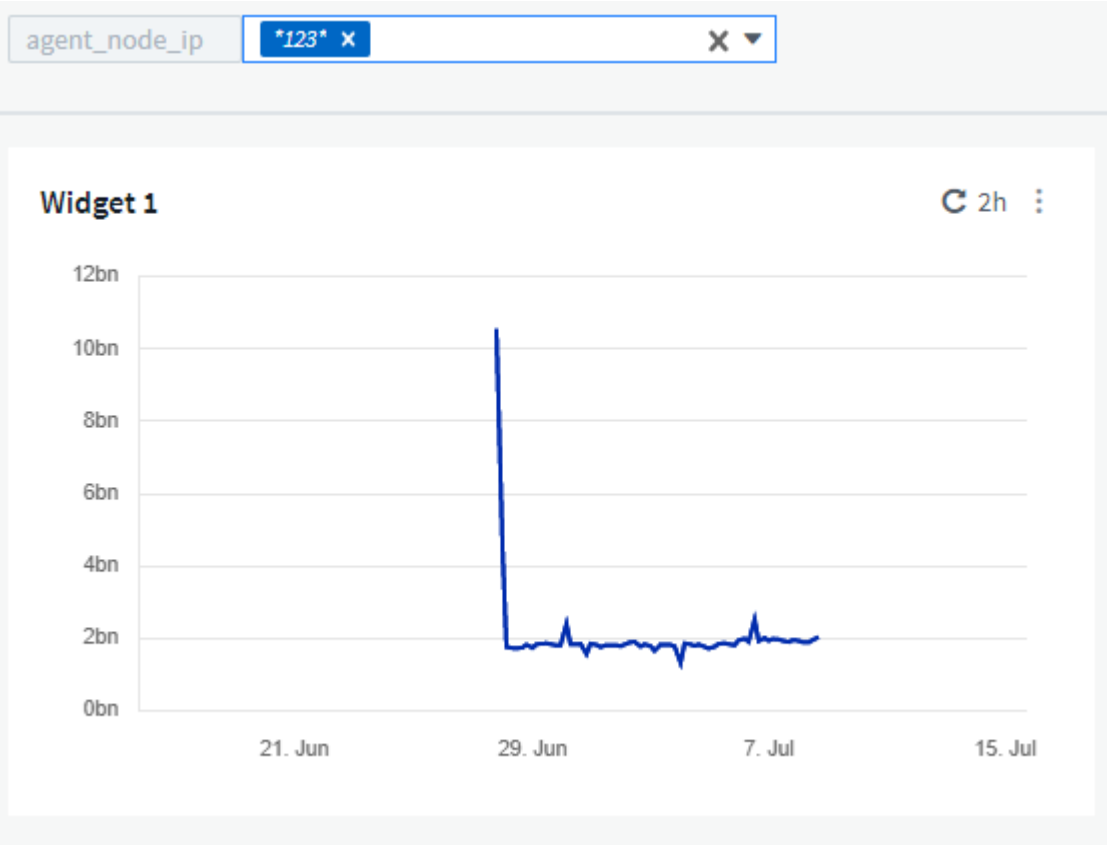


Variabili di attributo

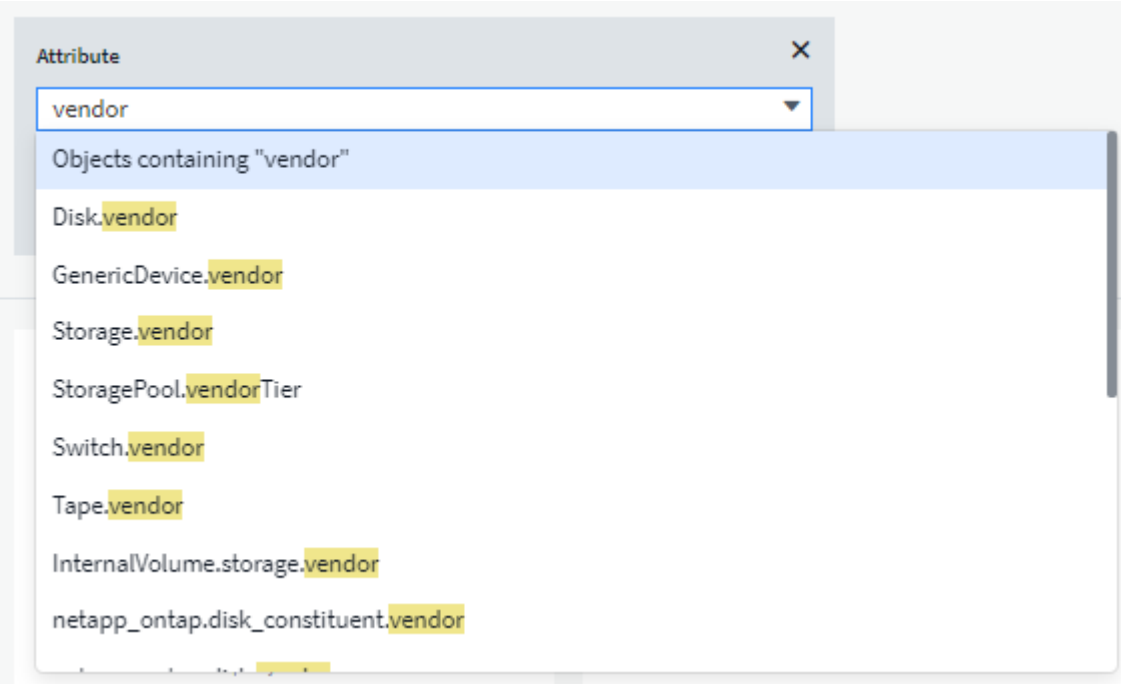
Selezionando una variabile di tipo Attributo è possibile filtrare i dati del widget contenenti il valore o i valori dell'attributo specificati. L'esempio seguente mostra un widget di linea che mostra le tendenze della memoria libera per i nodi Agent. Abbiamo creato una variabile per gli IP dei nodi agente, attualmente impostata per mostrare tutti gli IP:



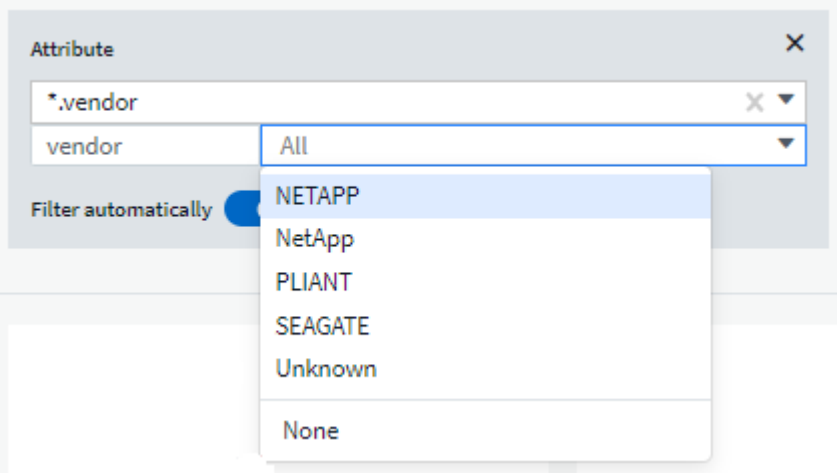
Tuttavia, se temporaneamente si desidera visualizzare solo i nodi su singole subnet del tenant, è possibile impostare o modificare la variabile su uno o più IP specifici del nodo agente. Qui stiamo visualizzando solo i nodi sulla subnet "123":



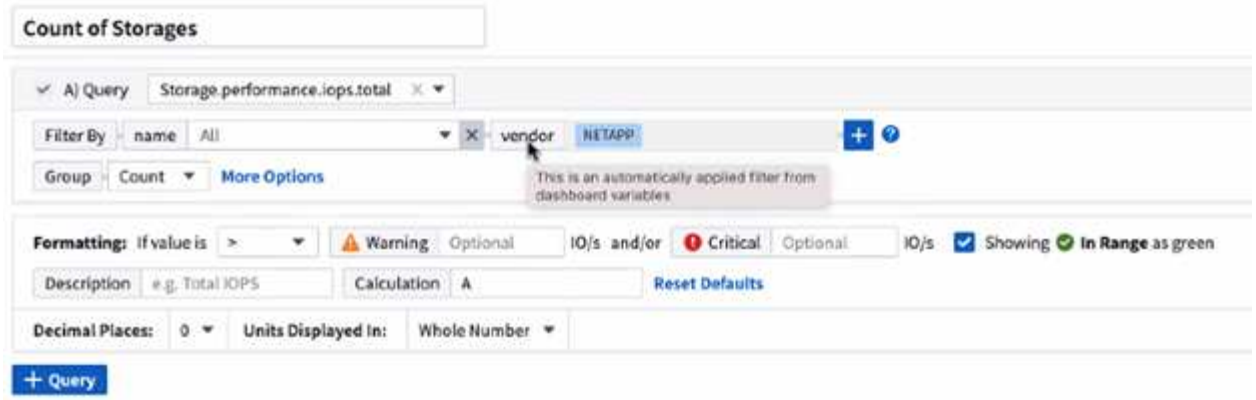
È anche possibile impostare una variabile per filtrare *tutti* gli oggetti con un attributo particolare, indipendentemente dal tipo di oggetto, ad esempio oggetti con un attributo "vendor", specificando **.vendor* nel campo variabile. Non è necessario digitare "*."; Data Infrastructure Insights lo fornirà se si seleziona l'opzione con caratteri jolly.



Quando si scorre l'elenco delle scelte per il valore della variabile, i risultati vengono filtrati in modo da mostrare solo i fornitori disponibili in base agli oggetti presenti nella dashboard.



Se modifichi un widget sulla tua dashboard in cui il filtro degli attributi è rilevante (ovvero, gli oggetti del widget contengono un attributo **.vendor*), ti verrà mostrato che il filtro degli attributi viene applicato automaticamente.

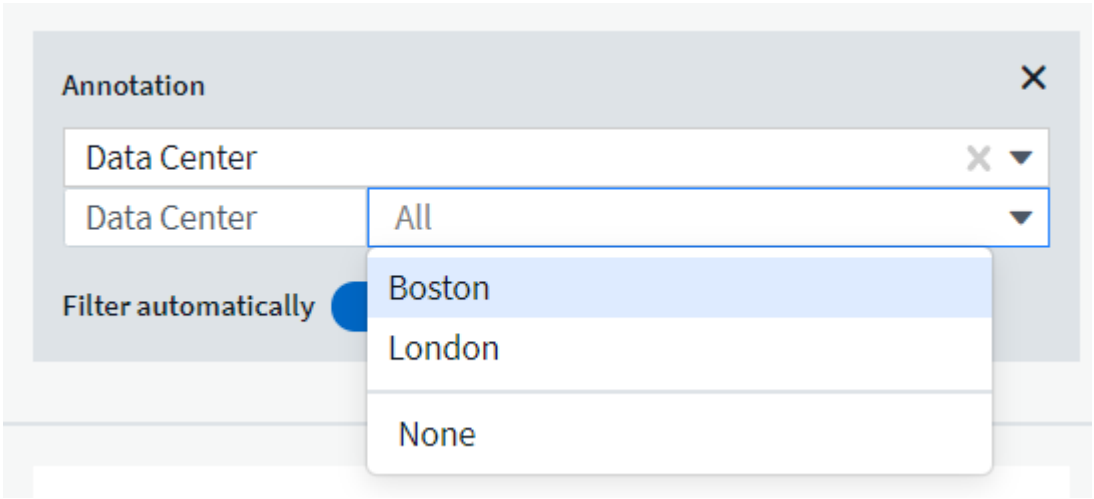


14

Applicare le variabili è semplice quanto modificare i dati degli attributi desiderati.

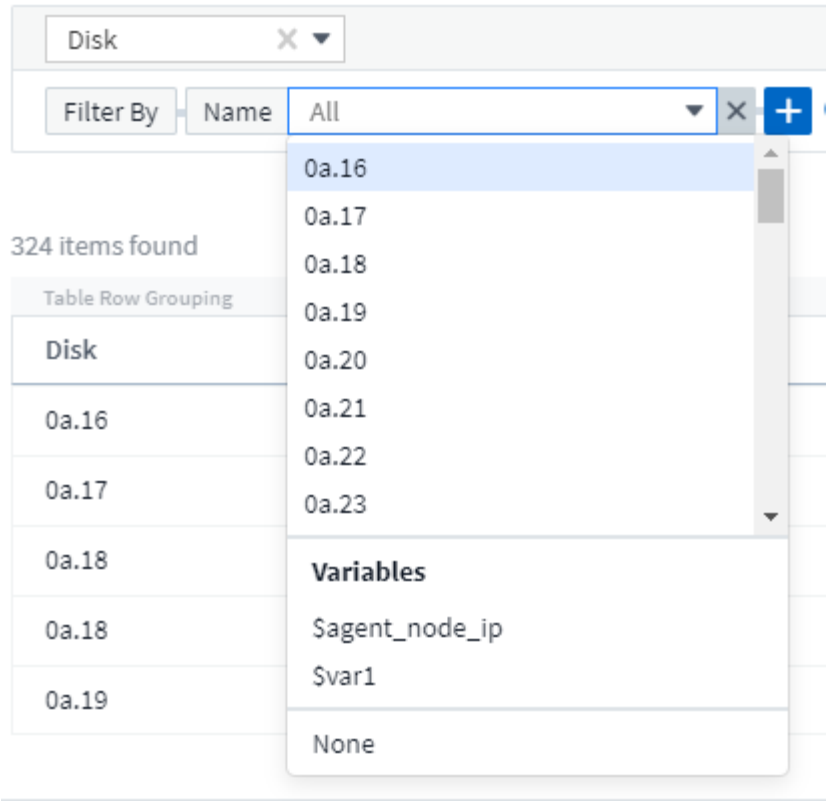
Variabili di annotazione

Scegliendo una variabile di annotazione è possibile filtrare gli oggetti associati a tale annotazione, ad esempio quelli appartenenti allo stesso Data Center.



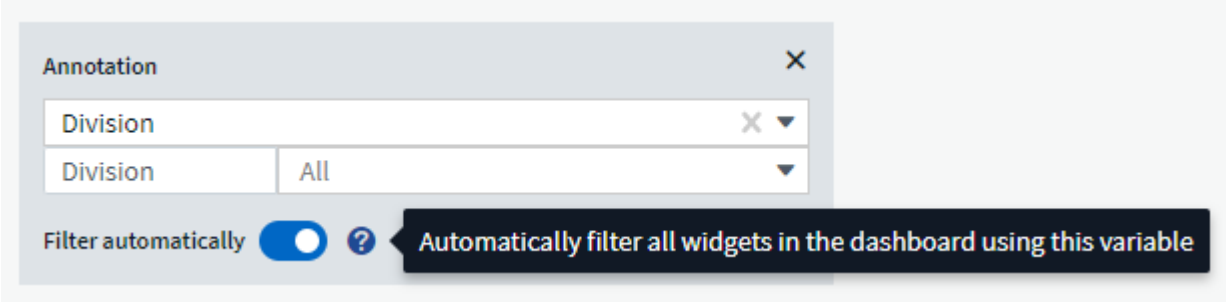
Variabile di testo, numero, data o booleana

È possibile creare variabili generiche non associate a un attributo particolare selezionando un tipo di variabile tra *Testo*, *Numero*, *Booleano* o *Data*. Una volta creata la variabile, è possibile selezionarla in un campo filtro del widget. Quando si imposta un filtro in un widget, oltre ai valori specifici che è possibile selezionare per il filtro, nell'elenco vengono visualizzate tutte le variabili create per la dashboard: queste sono raggruppate nella sezione "Variabili" nel menu a discesa e hanno nomi che iniziano con "$". Scegliendo una variabile in questo filtro potrai cercare i valori immessi nel campo variabile nella dashboard stessa. Tutti i widget che utilizzano quella variabile in un filtro verranno aggiornati dinamicamente.



Ambito del filtro variabile

Quando aggiungi una variabile Annotazione o Attributo alla dashboard, la variabile può essere applicata a *tutti* i widget sulla dashboard, il che significa che tutti i widget sulla dashboard visualizzeranno risultati filtrati in base al valore impostato nella variabile.



Si noti che solo le variabili Attributo e Annotazione possono essere filtrate automaticamente in questo modo. Le variabili non di annotazione o di attributo non possono essere filtrate automaticamente. Ogni singolo widget deve essere configurato per utilizzare variabili di questi tipi.

Per disattivare il filtro automatico in modo che la variabile venga applicata solo ai widget in cui è stata specificatamente impostata, fare clic sul cursore "Filtra automaticamente" per disattivarlo.

Per impostare una variabile in un singolo widget, apri il widget in modalità di modifica e seleziona l'annotazione o l'attributo specifico nel campo *Filtra per*. Con una variabile Annotazione, è possibile selezionare uno o più valori specifici oppure selezionare il nome della variabile (indicato dal simbolo "$" iniziale) per consentire la digitazione della variabile a livello di dashboard. Lo stesso vale per le variabili Attributo. Solo i widget per i quali hai impostato la variabile mostreranno i risultati filtrati.

Il filtraggio nelle variabili è *contestuale*; quando selezioni un valore o dei valori di filtro per una variabile, le altre

variabili nella tua pagina mostreranno solo i valori pertinenti a quel filtro. Ad esempio, quando si imposta un filtro variabile su uno specifico *Modello* di archiviazione, tutte le variabili impostate per filtrare per *Nome* di archiviazione mostreranno solo i valori rilevanti per quel Modello.

Per utilizzare una variabile in un'espressione, è sufficiente digitare il nome della variabile come parte dell'espressione, ad esempio *$var1 * 100*. Nelle espressioni è possibile utilizzare solo variabili numeriche. Non è possibile utilizzare variabili di annotazione o di attributo numeriche nelle espressioni.

Il filtraggio nelle variabili è *contestuale*; quando selezioni un valore o dei valori di filtro per una variabile, le altre variabili nella tua pagina mostreranno solo i valori pertinenti a quel filtro. Ad esempio, quando si imposta un filtro variabile su uno specifico *Modello* di archiviazione, tutte le variabili impostate per filtrare per *Nome* di archiviazione mostreranno solo i valori rilevanti per quel Modello.

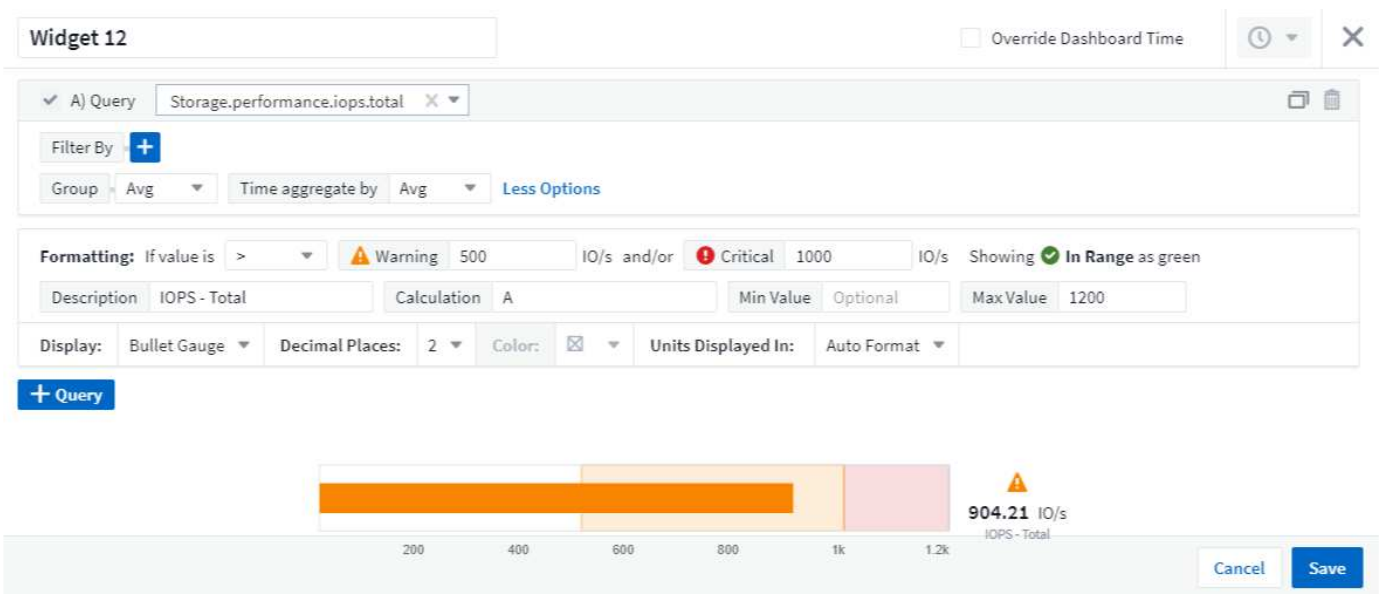
Denominazione delle variabili

Nomi delle variabili:

- Deve includere solo le lettere az, le cifre da 0 a 9, il punto (.), il trattino basso (_) e lo spazio ( ).
- Non può contenere più di 20 caratteri.
- Sono sensibili alle maiuscole e alle minuscole: $CityName e $cityname sono variabili diverse.
- Non può essere uguale al nome di una variabile esistente.
- Non può essere vuoto.

Formattazione dei widget degli indicatori

I widget Solid e Bullet Gauge consentono di impostare soglie per i livelli *Avviso* e/o *Critico*, fornendo una rappresentazione chiara dei dati specificati.



Per impostare la formattazione per questi widget, segui questi passaggi:

1. Scegli se vuoi evidenziare i valori maggiori (>) o minori (<) delle tue soglie. In questo esempio evidenzieremo i valori maggiori (>) dei livelli soglia.
2. Selezionare un valore per la soglia di "Avviso". Quando il widget visualizza valori superiori a questo livello, l'indicatore viene visualizzato in arancione.

3. Selezionare un valore per la soglia "Critica". I valori superiori a questo livello faranno sì che l'indicatore venga visualizzato in rosso.

Facoltativamente, è possibile scegliere un valore minimo e massimo per l'indicatore. I valori inferiori al minimo non visualizzeranno l'indicatore. I valori superiori al massimo visualizzeranno un indicatore pieno. Se non si selezionano valori minimi o massimi, il widget seleziona i valori minimi e massimi ottimali in base al valore del widget.

Formattazione del widget a valore singolo

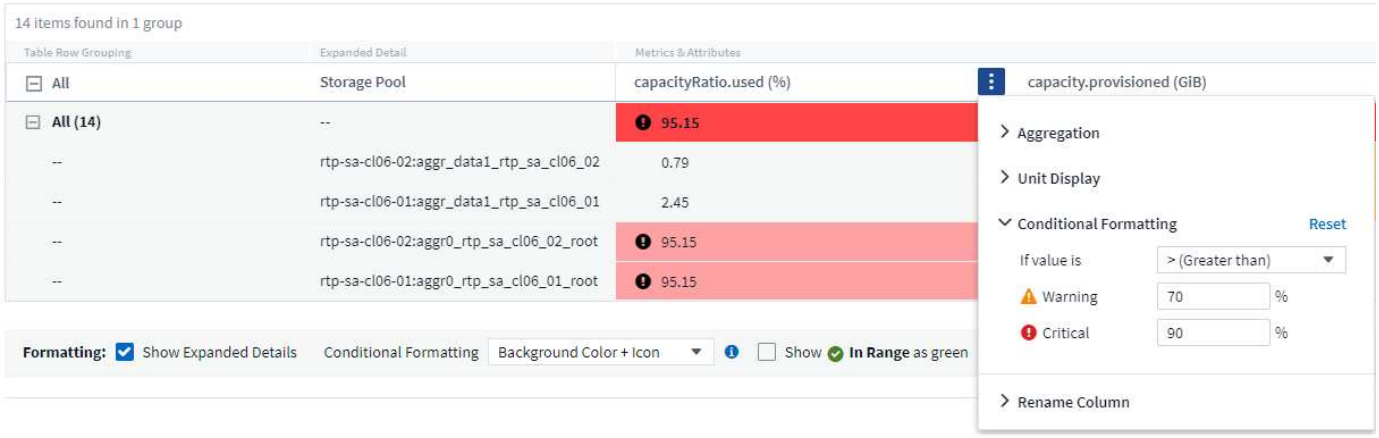
Nel widget Valore singolo, oltre a impostare le soglie di Avviso (arancione) e Critico (rosso), puoi scegliere di visualizzare i valori "Nell'intervallo" (quelli al di sotto del livello di Avviso) con sfondo verde o bianco.

Facendo clic sul collegamento in un widget a valore singolo o in un widget indicatore, verrà visualizzata una pagina di query corrispondente alla prima query nel widget.

Widget della tabella di formattazione

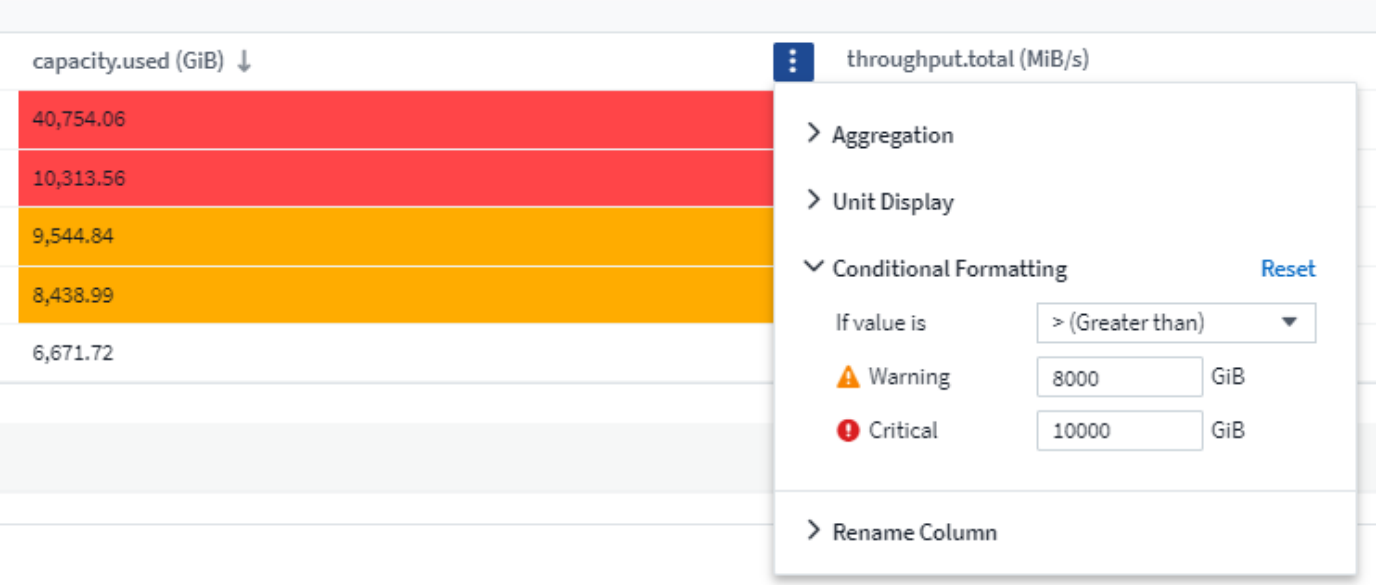
Analogamente ai widget a valore singolo e a indicatore, è possibile impostare la formattazione condizionale nei widget tabella, consentendo di evidenziare i dati con colori e/o icone speciali.

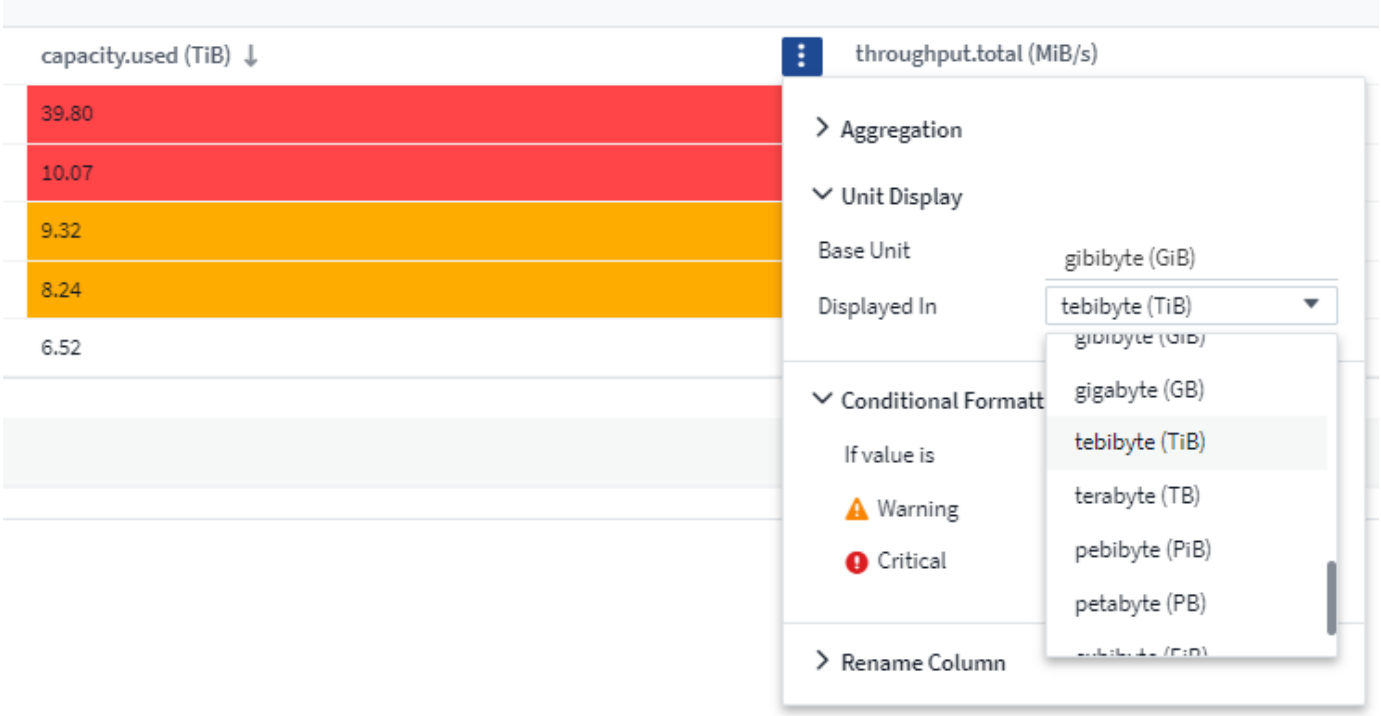
La formattazione condizionale consente di impostare ed evidenziare le soglie di livello di avviso e di livello critico nei widget della tabella, offrendo visibilità immediata ai valori anomali e ai punti dati eccezionali.



La formattazione condizionale viene impostata separatamente per ogni colonna di una tabella. Ad esempio, è possibile scegliere un set di soglie per una colonna di capacità e un altro set per una colonna di produttività.

Se si modifica la visualizzazione dell'unità per una colonna, la formattazione condizionale rimane invariata e riflette la modifica dei valori. Le immagini sottostanti mostrano la stessa formattazione condizionale anche se l'unità di visualizzazione è diversa.



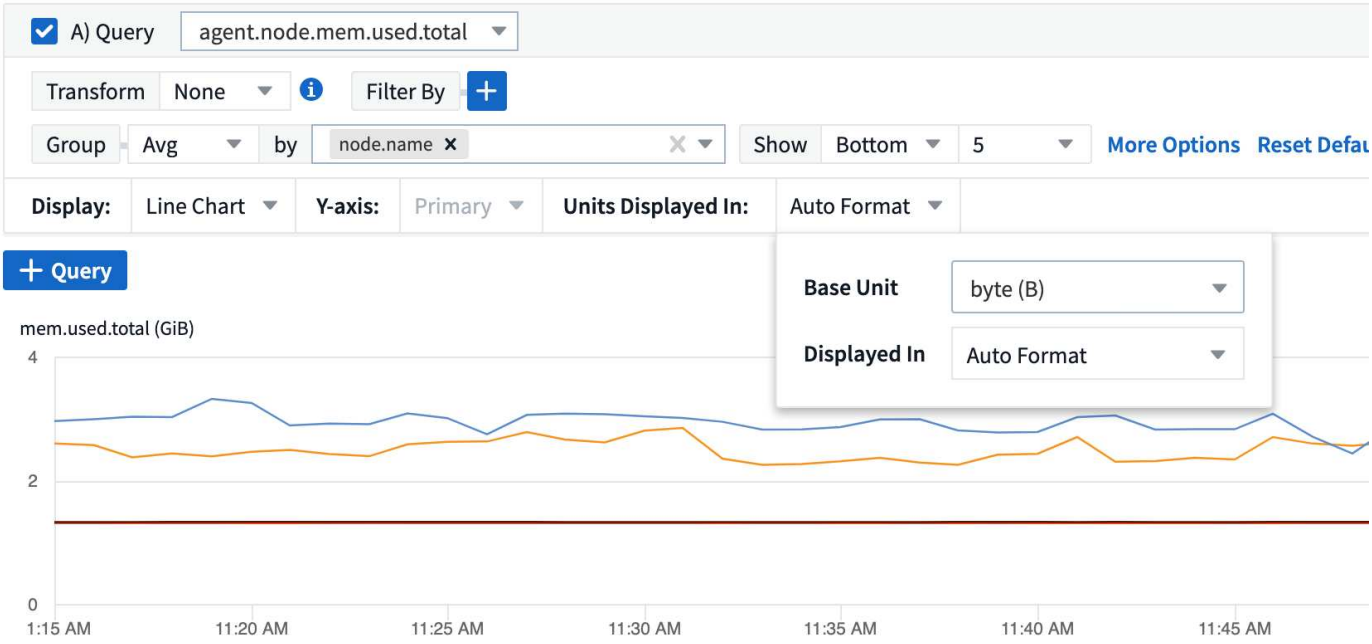


È possibile scegliere se visualizzare la formattazione delle condizioni come colore, come icone o come entrambi.

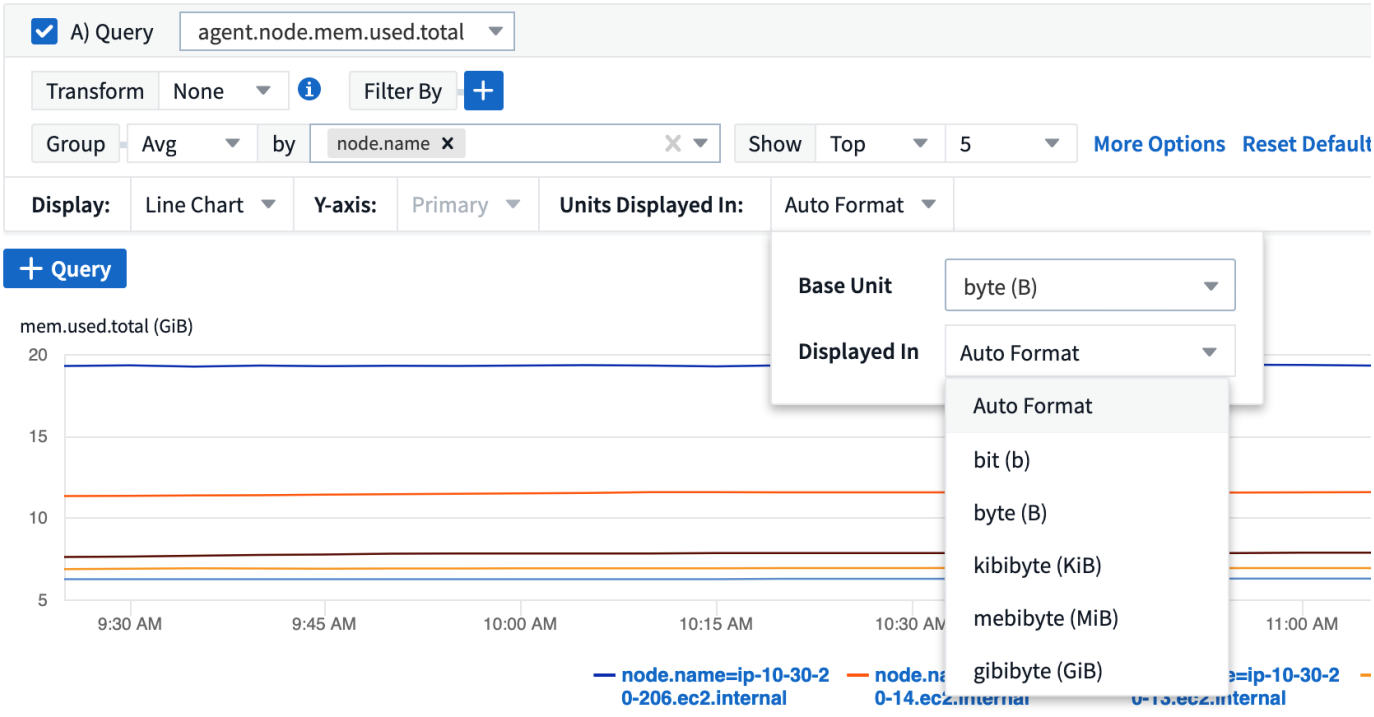
Scelta dell'unità per la visualizzazione dei dati

La maggior parte dei widget su una dashboard consente di specificare le unità in cui visualizzare i valori, ad esempio *Megabyte*, *Migliaia*, *Percentuale*, *Millisecondi (ms)*, ecc. In molti casi, Data Infrastructure Insights conosce il formato migliore per i dati acquisiti. Nei casi in cui non si conosce il formato migliore, è possibile impostare il formato desiderato.

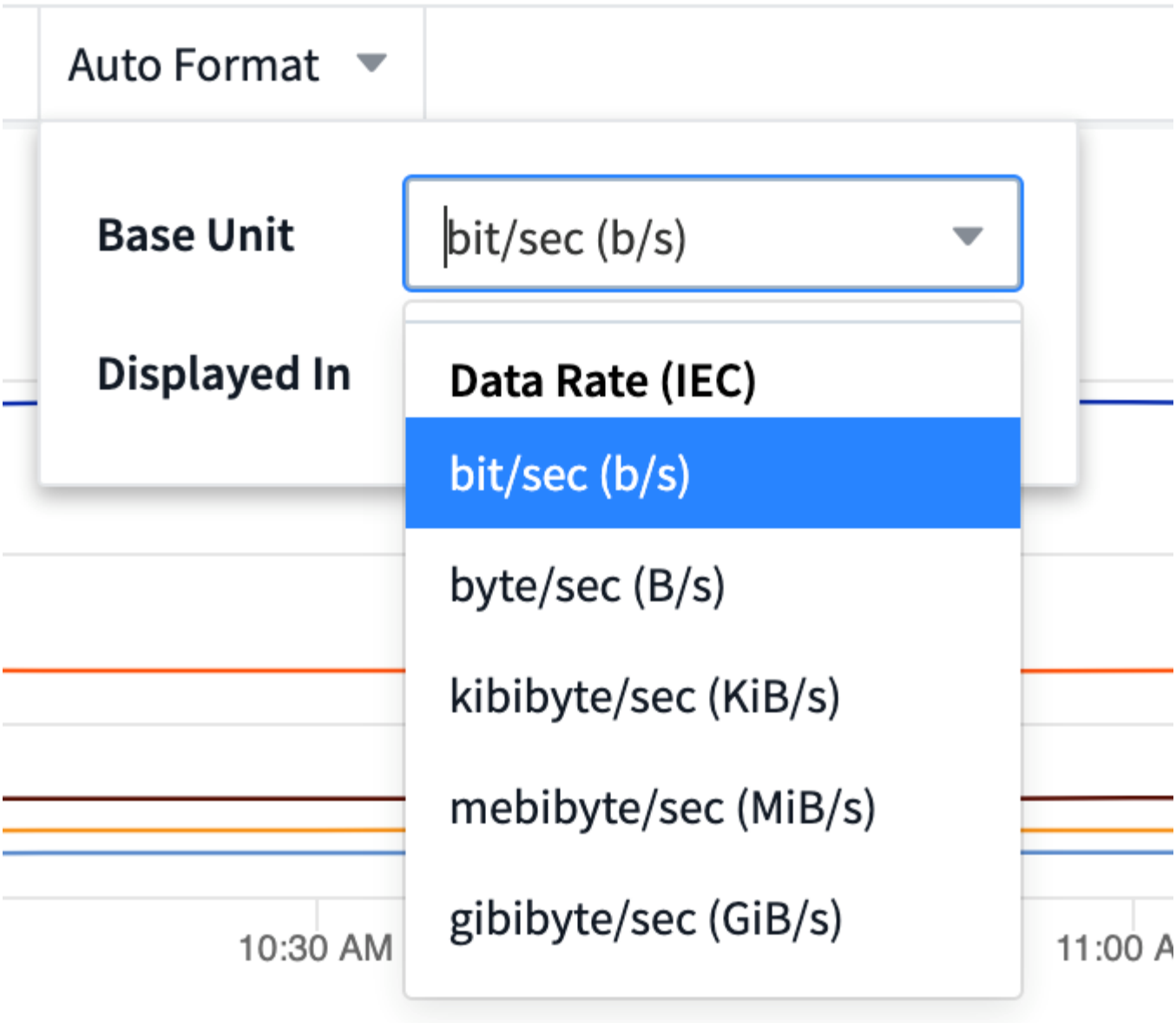
Nell'esempio di grafico a linee riportato di seguito, i dati selezionati per il widget sono in *byte* (l'unità di dati IEC di base: vedere la tabella seguente), quindi l'unità di base viene automaticamente selezionata come 'byte (B)'. Tuttavia, i valori dei dati sono sufficientemente grandi da essere presentati come gibibyte (GiB), pertanto Data Infrastructure Insights formatta automaticamente i valori come GiB per impostazione predefinita. L'asse Y del grafico mostra 'GiB' come unità di visualizzazione e tutti i valori sono visualizzati in termini di tale unità.



Se si desidera visualizzare il grafico in un'unità diversa, è possibile scegliere un altro formato in cui visualizzare i valori. Poiché l'unità di base in questo esempio è *byte*, è possibile scegliere tra i formati "basati su byte" supportati: bit (b), byte (B), kibibyte (KiB), mebibyte (MiB), gibibyte (GiB). L'etichetta e i valori dell'asse Y cambiano in base al formato scelto.



Nei casi in cui l'unità di base non è nota, è possibile assegnare un'unità tra le"unità disponibili" oppure digita il tuo nome. Dopo aver assegnato un'unità di base, è possibile scegliere di visualizzare i dati in uno dei formati supportati appropriati.



Per cancellare le impostazioni e ricominciare, clicca su **Ripristina impostazioni predefinite**.

Una parola sulla formattazione automatica

La maggior parte delle metriche viene segnalata dai raccoglitori di dati nell'unità più piccola, ad esempio come numero intero, ad esempio 1.234.567.890 byte. Per impostazione predefinita, Data Infrastructure Insights formatterà automaticamente il valore per la visualizzazione più leggibile. Ad esempio, un valore di dati pari a 1.234.567.890 byte verrebbe formattato automaticamente in 1,23 *Gibibyte*. Puoi scegliere di visualizzarlo in un altro formato, ad esempio *Mebibytes*. Il valore verrà visualizzato di conseguenza.

Data Infrastructure Insights utilizza gli standard di denominazione dei numeri in inglese americano. Il "miliardo" americano equivale a "mille milioni".

Widget con più query

Se si dispone di un widget di serie temporali (ad esempio linea, spline, area, area impilata) che ha due query in cui entrambe sono tracciate sull'asse Y primario, l'unità di base non viene visualizzata nella parte superiore dell'asse Y. Tuttavia, se il widget ha una query sull'asse Y primario e una query sull'asse Y secondario,

vengono visualizzate le unità di base per ciascuna.

Se il widget ha tre o più query, le unità di base non vengono visualizzate sull'asse Y.

Unità disponibili

Nella tabella seguente sono riportate tutte le unità disponibili per categoria.

Categoria	Unità
Valuta	centesimo di dollaro
Dati (IEC)	bit byte kibibyte mebibyte gibibyte tebibyte pebibyte exbibyte
Velocità dati (IEC)	bit/sec byte/sec kibibyte/sec mebibyte/sec gibibyte/sec tebibyte/sec pebibyte/sec
Dati (metrici)	kilobyte megabyte gigabyte terabyte petabyte exabyte
DataRate (metrico)	kilobyte/sec megabyte/sec gigabyte/sec terabyte/sec petabyte/sec exabyte/sec
CEI	kibi mebi gibi tebi pebi exbi
Decimale	numero intero mille milioni miliardi trilioni
Percentuale	percentuale
Tempo	nanosecondo microsecondo millisecondo secondo minuto ora
Temperatura	gradi Celsius Fahrenheit
Frequenza	hertz kilohertz megahertz gigahertz
processore	nanocore microcore millicore core kilocore megacore gigacore teracore petacore exacore
Capacità di elaborazione	Operazioni I/O/sec operazioni/sec richieste/sec letture/sec scritture/sec operazioni/min letture/min scritture/min

Modalità TV e aggiornamento automatico

I dati nei widget sulle dashboard e nelle landing page delle risorse si aggiornano automaticamente in base a un intervallo di aggiornamento determinato dall'intervallo di tempo selezionato per la dashboard. L'intervallo di aggiornamento dipende dal fatto che il widget sia una serie temporale (grafico a linee, spline, ad area, ad area impilata) o non una serie temporale (tutti gli altri grafici).

Intervallo di tempo della dashboard	Intervallo di aggiornamento delle serie temporali	Intervallo di aggiornamento non serie temporale
Ultimi 15 minuti	10 secondi	1 minuto
Ultimi 30 minuti	15 secondi	1 minuto
Ultimi 60 minuti	15 secondi	1 minuto
Ultime 2 ore	30 secondi	5 minuti
Ultime 3 ore	30 secondi	5 minuti
Ultime 6 ore	1 minuto	5 minuti
Ultime 12 ore	5 minuti	10 minuti
Ultime 24 ore	5 minuti	10 minuti
Ultimi 2 giorni	10 minuti	10 minuti
Ultimi 3 giorni	15 minuti	15 minuti
Ultimi 7 giorni	1 ora	1 ora
Ultimi 30 giorni	2 ore	2 ore

Ogni widget visualizza il proprio intervallo di aggiornamento automatico nell'angolo in alto a destra del widget.

L'aggiornamento automatico non è disponibile per l'intervallo di tempo della dashboard personalizzata.

Se abbinato alla **Modalità TV**, l'aggiornamento automatico consente la visualizzazione dei dati in tempo quasi reale su una dashboard o una pagina di risorse. La modalità TV offre una visualizzazione ordinata; il menu di navigazione è nascosto, lasciando più spazio sullo schermo per la visualizzazione dei dati, così come il pulsante Modifica. La modalità TV ignora i tipici timeout Data Infrastructure Insights , lasciando attiva la visualizzazione finché non si esegue la disconnessione manuale o automatica tramite protocolli di sicurezza di autorizzazione.

Poiché NetApp Console ha un timeout di accesso utente di 7 giorni, anche Data Infrastructure Insights deve disconnettersi in base a tale evento. Puoi semplicemente effettuare nuovamente l'accesso e la tua dashboard continuerà a essere visualizzata.

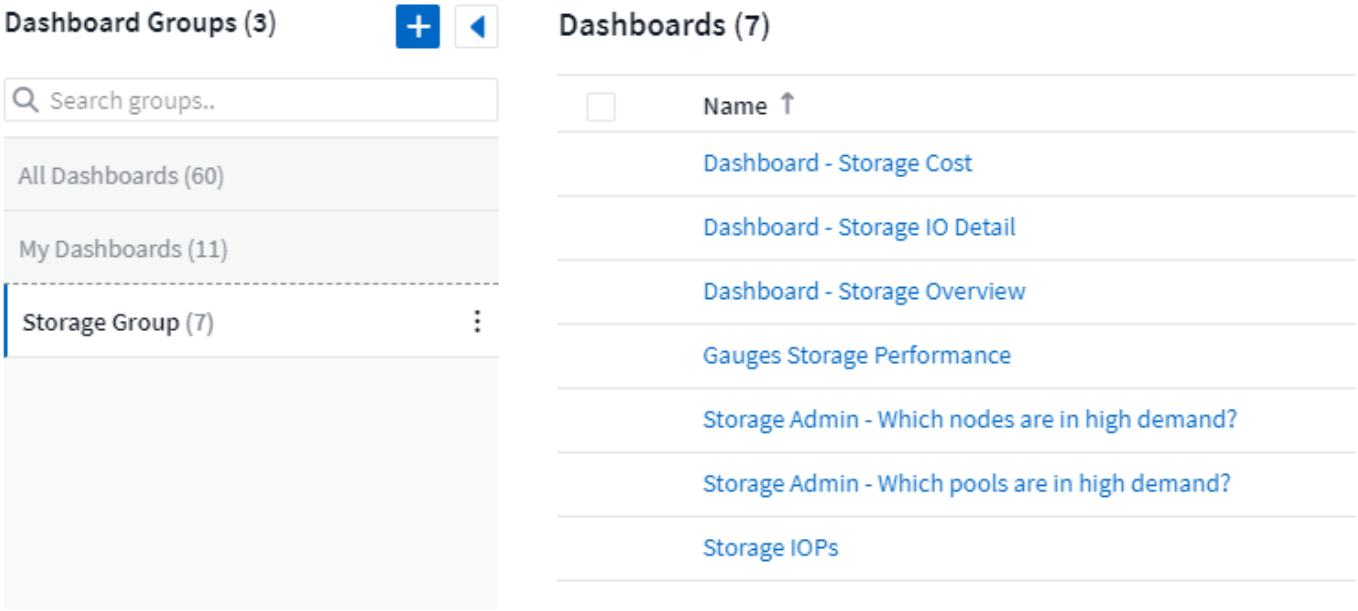
- Per attivare la modalità TV, fare clic sul pulsante Modalità TV.
- Per disattivare la modalità TV, fare clic sul pulsante **Esci** in alto a sinistra dello schermo.

È possibile sospendere temporaneamente l'aggiornamento automatico facendo clic sul pulsante Pausa nell'angolo in alto a destra. Durante la pausa, il campo dell'intervallo di tempo della dashboard visualizzerà l'intervallo di tempo attivo dei dati in pausa. I tuoi dati continuano ad essere acquisiti e aggiornati anche se l'aggiornamento automatico è in pausa. Fare clic sul pulsante Riprendi per continuare l'aggiornamento automatico dei dati.

Gruppi della dashboard

Il raggruppamento consente di visualizzare e gestire dashboard correlate. Ad esempio, puoi avere un gruppo dashboard dedicato allo storage del tuo tenant. I gruppi di dashboard vengono gestiti nella pagina **Dashboard**

> Mostra tutte le dashboard.



Per impostazione predefinita vengono visualizzati due gruppi:

- **Tutte le dashboard** elenca tutte le dashboard create, indipendentemente dal proprietario.
- **Le mie dashboard** elenca solo le dashboard create dall'utente corrente.

Il numero di dashboard contenute in ciascun gruppo è indicato accanto al nome del gruppo.

Per creare un nuovo gruppo, fare clic sul pulsante **"+" Crea nuovo gruppo dashboard**. Inserisci un nome per il gruppo e clicca su **Crea gruppo**. Viene creato un gruppo vuoto con quel nome.

Per aggiungere dashboard al gruppo, fai clic sul gruppo *Tutte le dashboard* per visualizzare tutte le dashboard del tuo tenant oppure fai clic su *Le mie dashboard* se desideri visualizzare solo le dashboard di tua proprietà ed esegui una delle seguenti operazioni:

- Per aggiungere una singola dashboard, fare clic sul menu a destra della dashboard e selezionare *Aggiungi al gruppo*.
- Per aggiungere più dashboard a un gruppo, selezionale facendo clic sulla casella di controllo accanto a ciascuna dashboard, quindi fai clic sul pulsante **Azioni in blocco** e seleziona *Aggiungi al gruppo*.

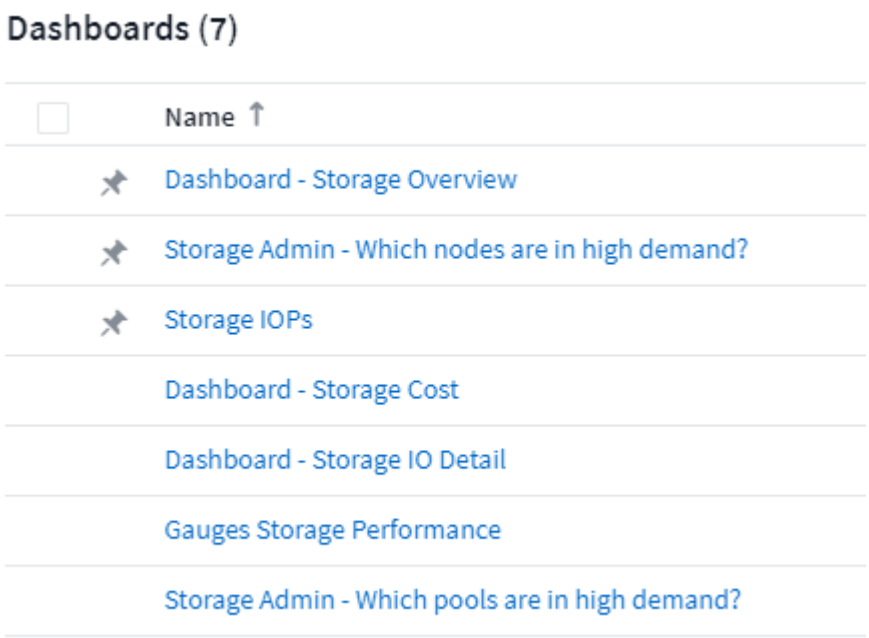
Rimuovere le dashboard dal gruppo corrente nello stesso modo selezionando *Rimuovi dal gruppo*. Non è possibile rimuovere dashboard dal gruppo *Tutte le dashboard* o *Le mie dashboard*.

> La rimozione di una dashboard da un gruppo non elimina la dashboard da Data Infrastructure Insights. Per rimuovere completamente una dashboard, selezionala e fai clic su *Elimina*. In questo modo l'utente verrà rimosso da tutti i gruppi a cui apparteneva e non sarà più disponibile per nessun altro utente.

Aggiungi ai preferiti i tuoi dashboard

Puoi gestire ulteriormente le tue dashboard aggiungendo quelle preferite in cima all'elenco delle dashboard. Per aggiungere una dashboard, è sufficiente fare clic sul pulsante a forma di puntina da disegno visualizzato quando si passa il mouse su una dashboard in qualsiasi elenco.

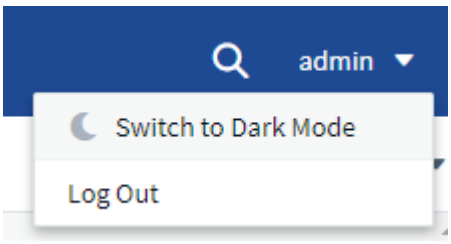
La possibilità di aggiungere/rimuovere la dashboard è una preferenza individuale dell'utente e indipendente dal gruppo (o dai gruppi) a cui appartiene la dashboard.



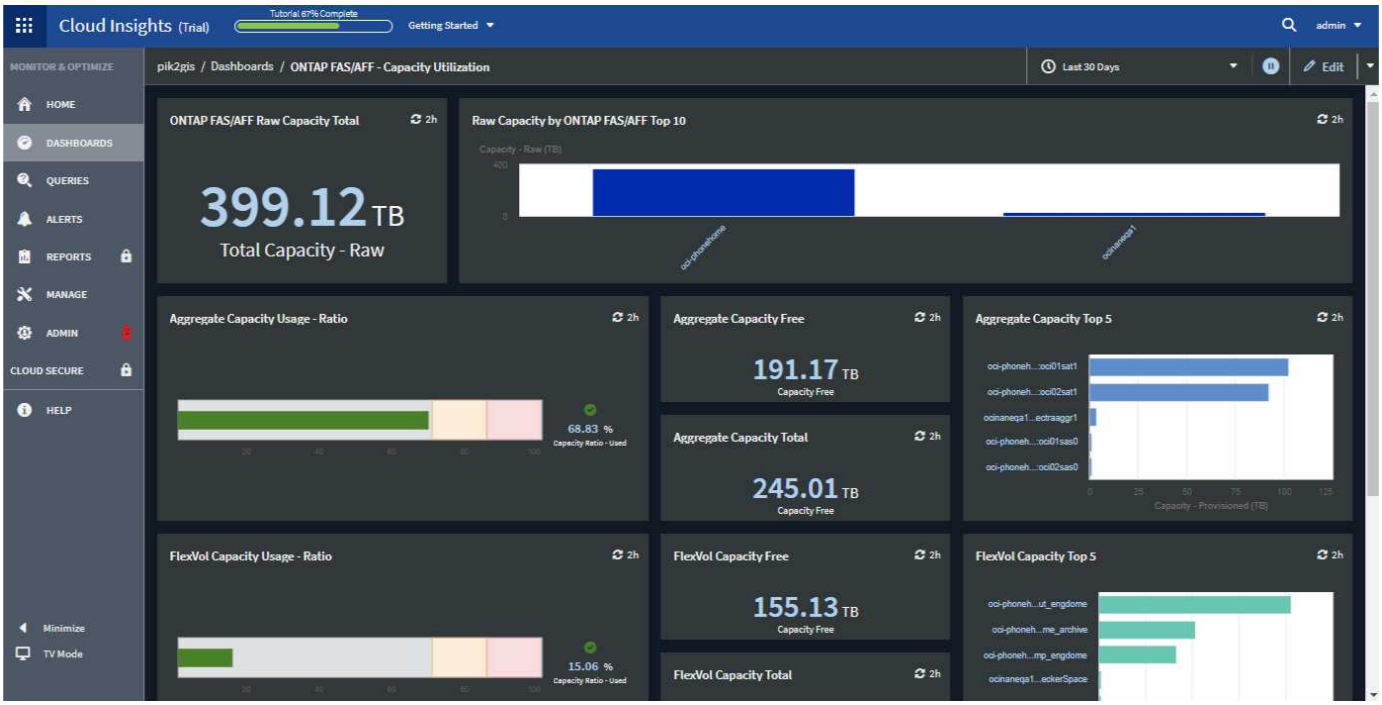
Tema scuro

È possibile scegliere di visualizzare Data Infrastructure Insights utilizzando un tema chiaro (predefinito), che visualizza la maggior parte delle schermate con uno sfondo chiaro e testo scuro, oppure un tema scuro, che visualizza la maggior parte delle schermate con uno sfondo scuro e testo chiaro.

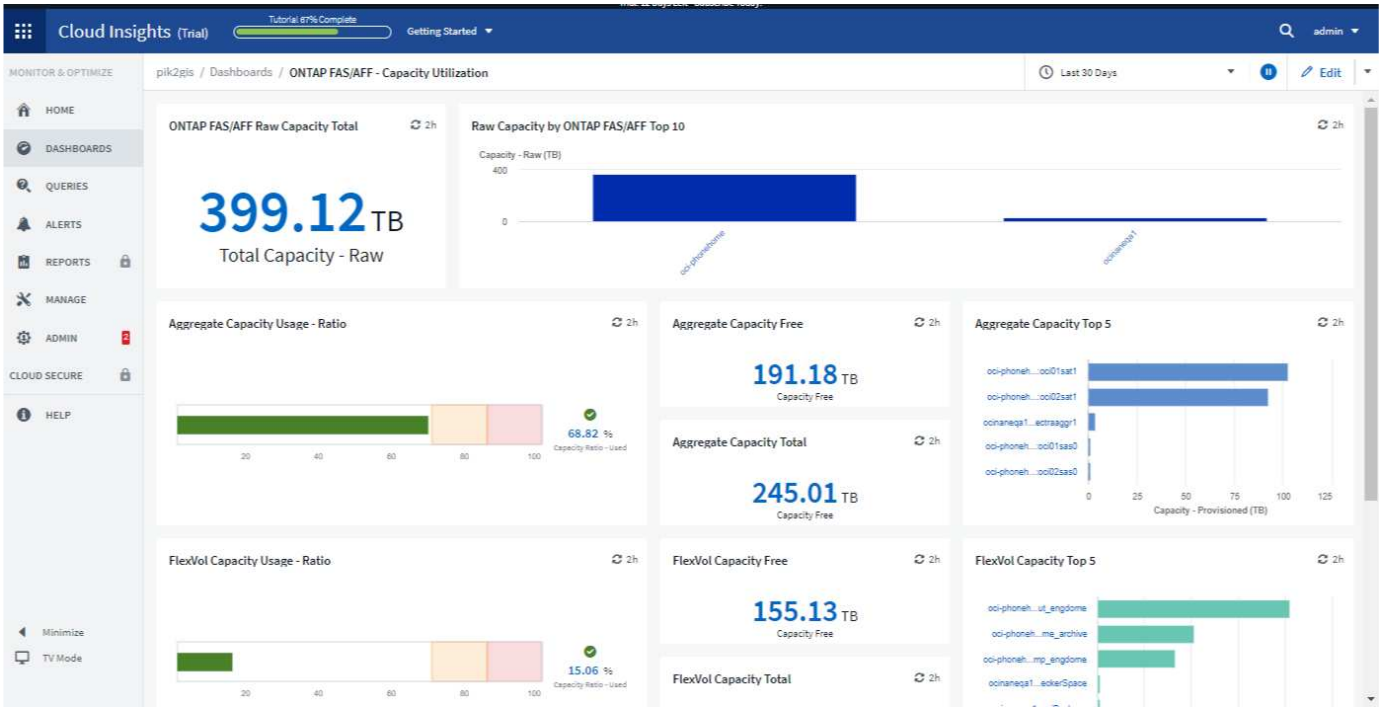
Per passare dal tema chiaro a quello scuro, clicca sul pulsante del nome utente nell'angolo in alto a destra dello schermo e scegli il tema desiderato.



Visualizzazione dashboard tema scuro:



Visualizzazione dashboard tema chiaro:



Alcune aree dello schermo, come alcuni grafici dei widget, mostrano comunque sfondi chiari anche se visualizzati con il tema scuro.

Interpolazione del grafico lineare

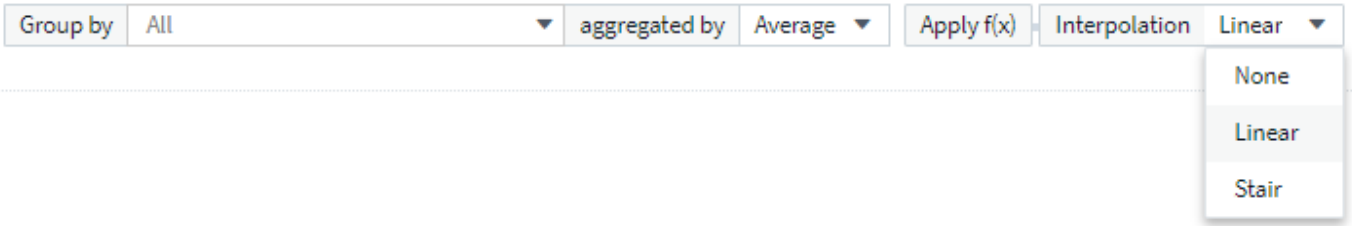
Spesso i diversi raccoglitori di dati interrogano i propri dati a intervalli diversi. Ad esempio, il raccoglitore di dati A può effettuare il polling ogni 15 minuti, mentre il raccoglitore di dati B può effettuarlo ogni cinque minuti. Quando un widget grafico a linee (anche grafici spline, ad area e ad area impilata) aggrega questi dati da più collettori di dati in un'unica riga (ad esempio, quando il widget raggruppa per "tutto") e aggiorna la riga ogni

cinque minuti, i dati del collettore B potrebbero essere visualizzati in modo accurato, mentre i dati del collettore A potrebbero presentare delle lacune, influenzando così l'aggregazione finché il collettore A non esegue nuovamente il polling.

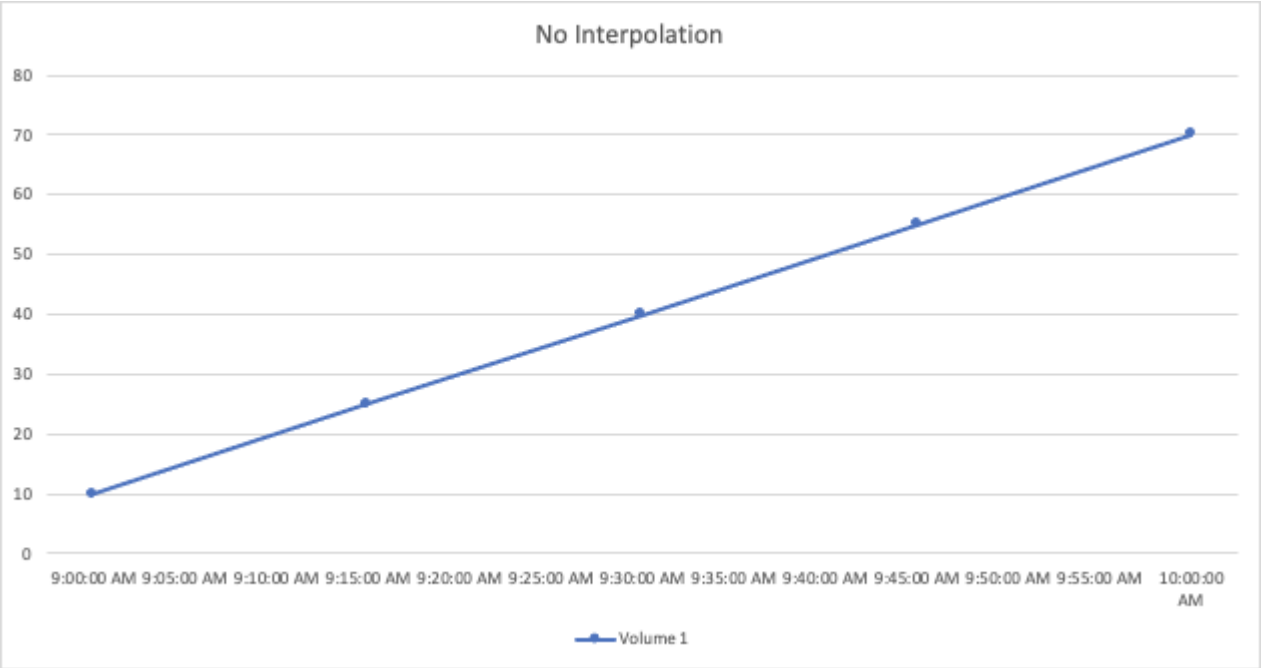
Per ovviare a questo problema, Data Infrastructure Insights interpola i dati durante l'aggregazione, utilizzando i punti dati circostanti per effettuare una "stima migliore" dei dati finché i raccoglitori di dati non eseguono nuovamente il polling. È sempre possibile visualizzare singolarmente i dati degli oggetti di ciascun raccoglitore dati modificando il raggruppamento del widget.

Metodi di interpolazione

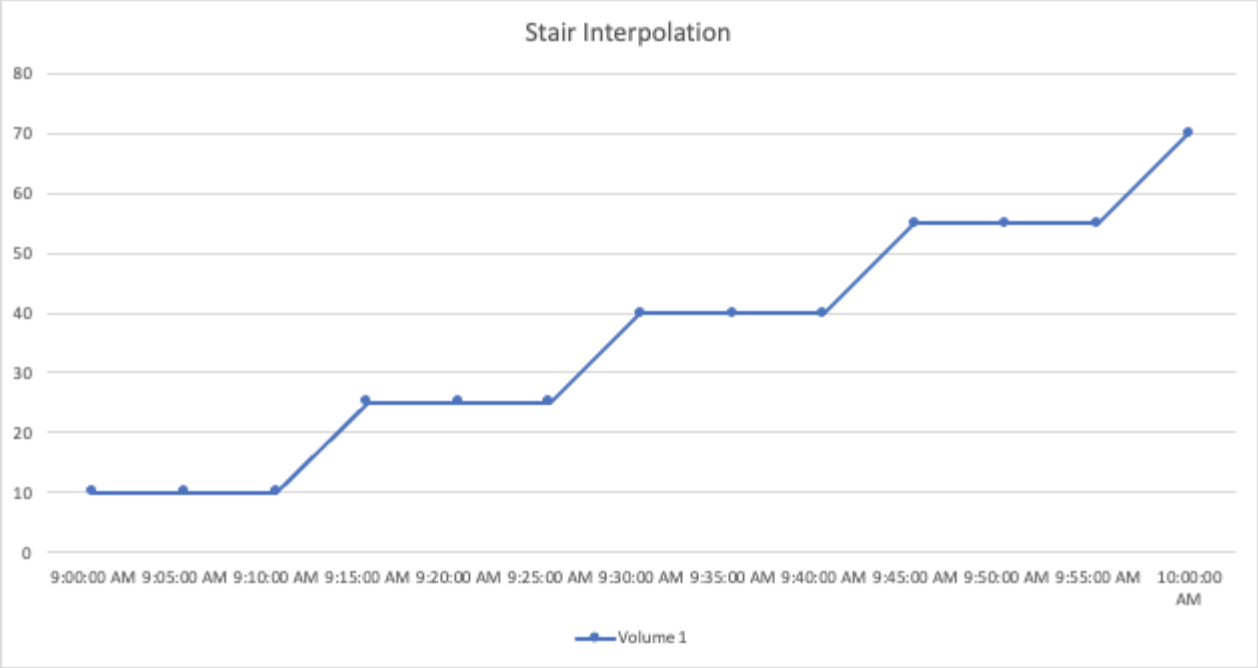
Quando si crea o si modifica un grafico a linee (oppure un grafico spline, ad area o ad area impilata), è possibile impostare il metodo di interpolazione su uno dei tre tipi. Nella sezione "Raggruppa per", seleziona l'interpolazione desiderata.



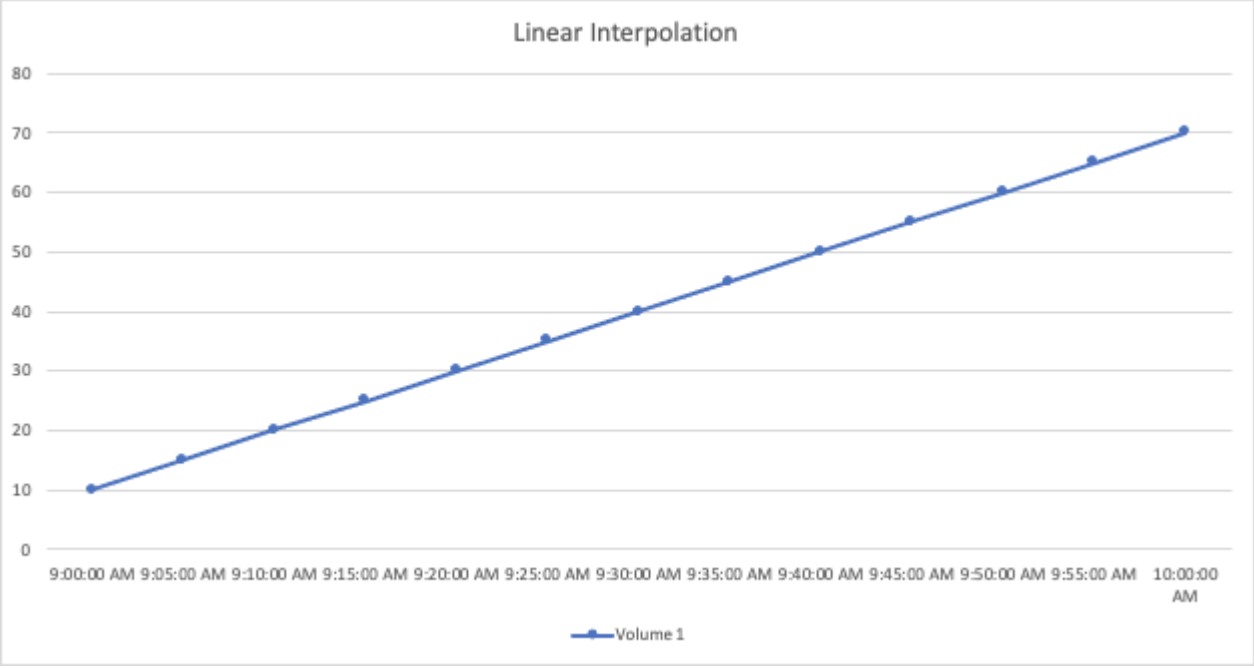
- **Nessuno**: non fare nulla, ovvero non generare punti intermedi.



- **Scala**: Un punto viene generato dal valore del punto precedente. In linea retta, questo apparirebbe come una tipica disposizione a "scala".



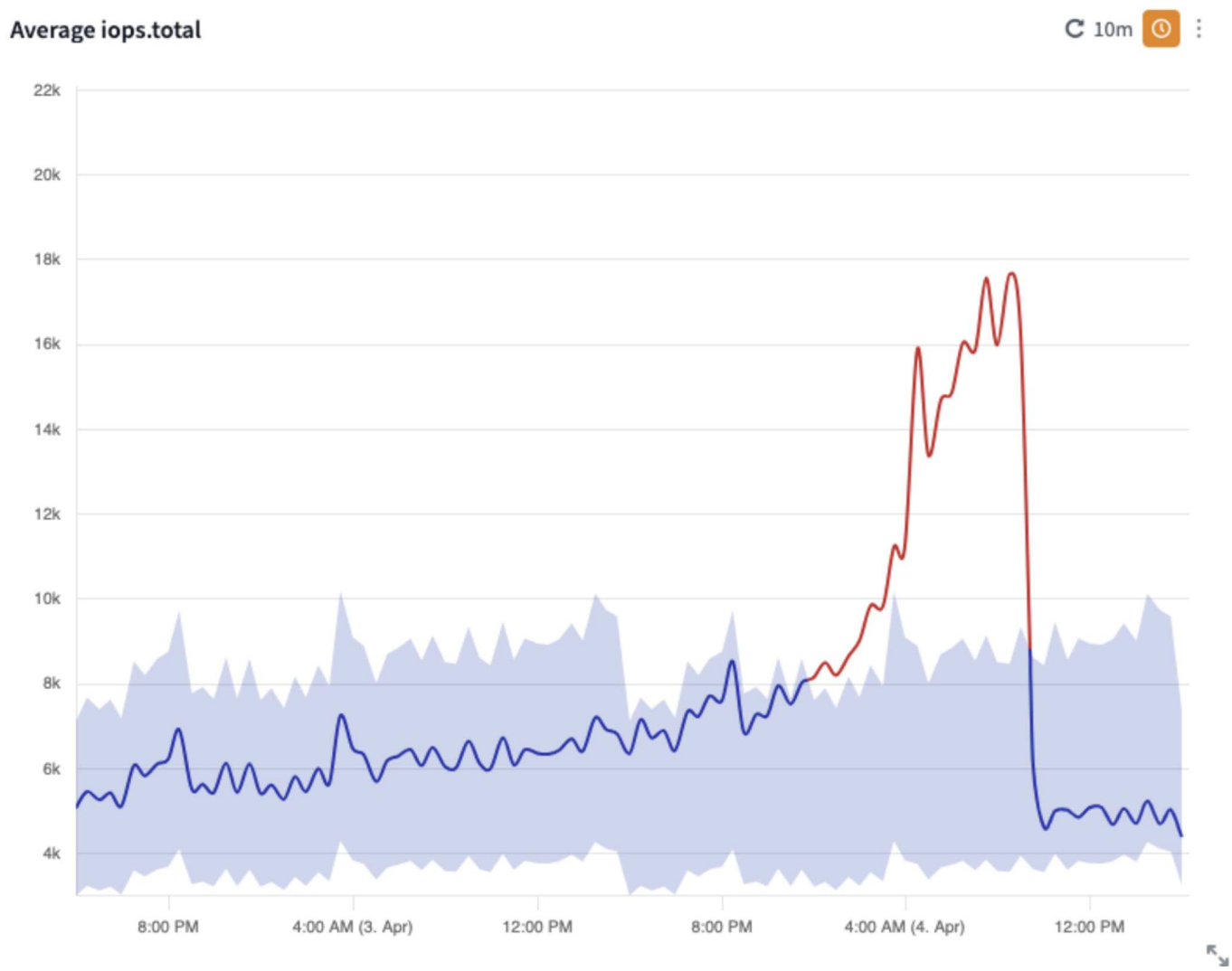
- **Lineare**: un punto viene generato come valore intermedio tra i due punti che collegano. Genera una linea simile alla linea che collega i due punti, ma con punti dati aggiuntivi (interpolati).



Limiti di anomalia nei widget di linea

Quando si include un widget grafico a linee o spline in una dashboard o in una landing page, è possibile scegliere di visualizzare il grafico nel contesto dei **limiti previsti** per i dati. Si può pensare a questo come alla ricerca di anomalie nei modelli dei dati.

DII utilizza dati stagionali (orari o giornalieri) per stabilire limiti superiori e inferiori rispetto a dove *si* aspetta_ che i dati si collochino in un dato momento. Se i dati superano o scendono al di sotto dei limiti previsti, il grafico evidenzierà tale anomalia.



Per visualizzare i limiti delle anomalie, modifica il widget e seleziona *Mostra limiti delle anomalie*. È possibile scegliere tra due algoritmi di rilevamento:

- **Adaptive Detector** si adatta rapidamente ai cambiamenti, rendendolo utile per indagini dettagliate.
- **Smooth Detector** riduce al minimo il rumore e i falsi positivi, filtrando le fluttuazioni a breve termine e continuando a rilevare spostamenti significativi.

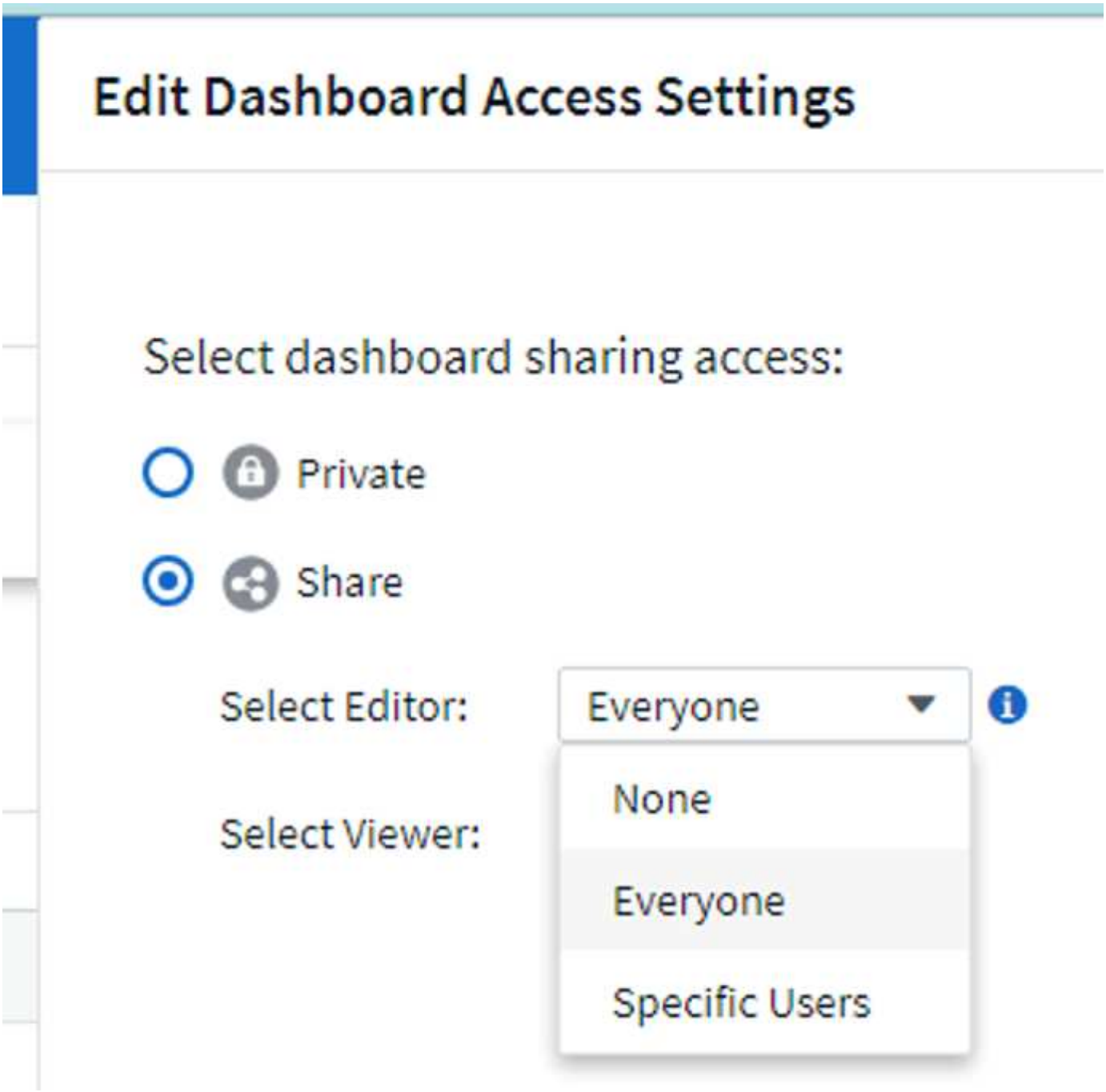
Inoltre, puoi scegliere di mostrare la stagionalità *Oraria* o *Giornaliera*, nonché impostare la sensibilità del rilevamento. Una sensibilità *alta* rileva più attraversamenti di confine, una sensibilità *bassa* ne rileva meno.

Tieni presente che potresti visualizzare solo i limiti previsti quando il grafico è impostato per visualizzare una singola linea. Se le impostazioni o i filtri di Raggruppa per mostrano più righe, oppure se hai impostato più query per il widget, l'opzione per mostrare i limiti previsti sarà disabilitata.

Gestione degli accessi alla dashboard

Data Infrastructure Insights ora ti offre un maggiore controllo sull'accesso alle dashboard

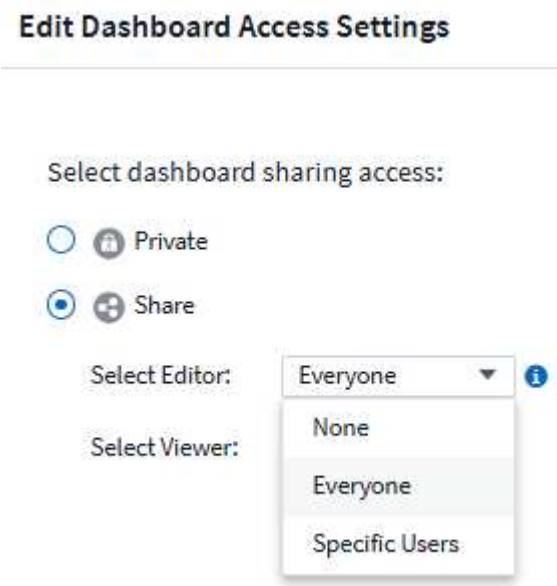
che crei. Puoi scegliere chi può modificare i tuoi grafici. Puoi controllare l'esposizione a informazioni potenzialmente sensibili. Mantenere una dashboard privata ti consente di finalizzare le tue visualizzazioni finché non saranno pronte per essere utilizzate da altri nella tua organizzazione.



Per impostazione predefinita, quando crei una nuova dashboard, questa è visibile solo a te, il creatore. Nessun altro utente può vedere o modificare la dashboard.

Una volta completata la dashboard, puoi scegliere di consentire ad altri membri della tua organizzazione di visualizzarla. Per condividere una dashboard, nell'elenco delle dashboard, seleziona *Condividi* dal menu a destra.

Puoi scegliere di condividere la dashboard con tutti o di selezionare solo gli utenti, con autorizzazioni di modifica o di sola lettura.



Best Practice per Dashboard e Widget

Suggerimenti e trucchi per aiutarti a sfruttare al meglio le potenti funzionalità di dashboard e widget.

Trovare la metrica giusta

Data Infrastructure Insights acquisisce contatori e metriche utilizzando nomi che a volte variano da un raccoglitore di dati all'altro.

Quando cerchi la metrica o il contatore giusto per il widget della dashboard, tieni presente che la metrica desiderata potrebbe avere un nome diverso da quello che stai pensando. Sebbene gli elenchi a discesa in Data Infrastructure Insights siano solitamente in ordine alfabetico, a volte un termine potrebbe non comparire nell'elenco dove ritieni che dovrebbe. Ad esempio, termini come "capacità grezza" e "capacità utilizzata" non compaiono insieme nella maggior parte degli elenchi.

Migliore pratica: usa la funzione di ricerca in campi come Filtra per o in posizioni come il selettore di colonna per trovare ciò che stai cercando. Ad esempio, cercando "cap" verranno mostrate tutte le metriche che contengono "capacità" nel nome, indipendentemente dalla loro posizione nell'elenco. Puoi quindi selezionare facilmente le metriche che desideri dall'elenco più breve.

Ecco alcune frasi alternative che puoi provare quando cerchi le metriche:

Quando vuoi trovare:	Prova anche a cercare:
processore	Processore
Capacità	Capacità utilizzata Capacità grezza Capacità fornita Capacità dei pool di archiviazione Capacità <altro tipo di risorsa> Capacità scritta
Velocità del disco	Velocità del disco più bassa Tipo di disco meno performante
Ospite	Host dell'hypervisor
Ipervisore	L'host è un hypervisor
Microcodice	Firmware
Nome	Alias Nome hypervisor Nome storage <altro tipo di asset> Nome semplice Nome risorsa Fabric Alias
Leggere/scrivere	Scrittura parziale R/W Scritture in sospeso IOPS - Scrittura Capacità scritta Latenza - Lettura Utilizzo della cache - lettura
Macchina virtuale	VM è virtuale

Questo non è un elenco esaustivo. Questi sono solo esempi di possibili termini di ricerca.

Trovare le risorse giuste

Le risorse a cui è possibile fare riferimento nei filtri e nelle ricerche dei widget variano a seconda del tipo di risorsa.

Nelle dashboard e nelle pagine delle risorse, il tipo di risorsa attorno al quale si sta creando il widget determina gli altri contatori dei tipi di risorsa per i quali è possibile filtrare o aggiungere una colonna. Quando crei il tuo widget, tieni presente quanto segue:

Questo tipo di risorsa/contatore:	È possibile filtrare in base a queste risorse:
Macchina virtuale	VMDK
Archivio dati	Volume interno VMDK Volume macchina virtuale
Ipervisore	La macchina virtuale è l'host dell'hypervisor
Ospite(i)	Volume interno Volume Cluster Host Macchina virtuale
Tessuto	Porta

Questo non è un elenco esaustivo.

Migliore pratica: se si sta filtrando per un tipo di risorsa specifico che non compare nell'elenco, provare a creare la query attorno a un tipo di risorsa alternativo.

Esempio di diagramma di dispersione: conoscere il proprio asse

La modifica dell'ordine dei contatori in un widget del grafico a dispersione modifica gli assi su cui vengono visualizzati i dati.

Informazioni su questo compito

Questo esempio creerà un grafico a dispersione che consentirà di visualizzare le VM con prestazioni inferiori e latenza elevata rispetto a quelle con IOPS bassi.

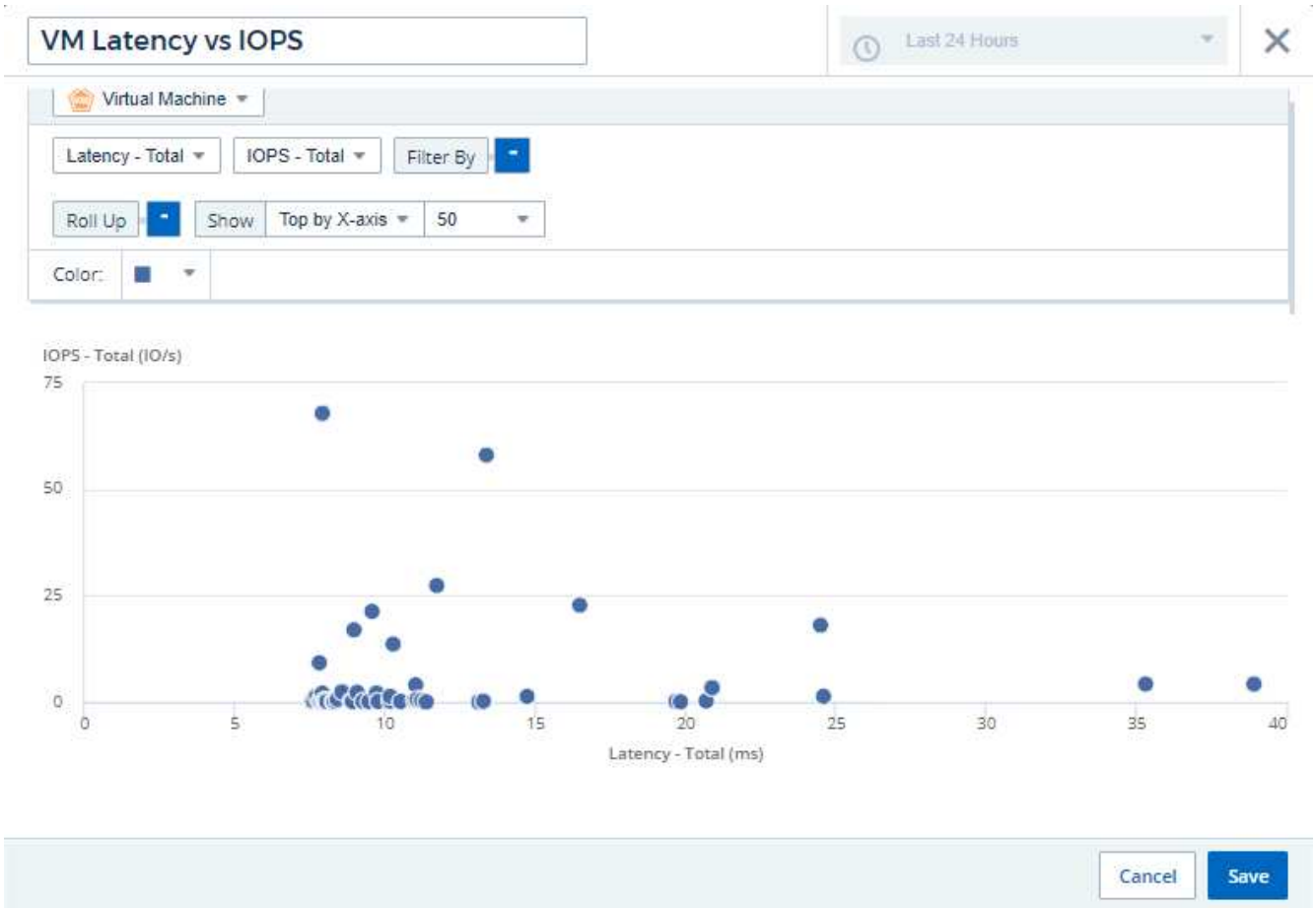
Passi

1. Crea o apri una dashboard in modalità di modifica e aggiungi un widget **Grafico a dispersione**.
2. Selezionare un tipo di risorsa, ad esempio *Macchina virtuale*.
3. Seleziona il primo contatore che desideri tracciare. Per questo esempio, selezionare *Latenza - Totale*.

   Latenza - Totale è rappresentata graficamente lungo l'asse X del grafico.

4. Seleziona il secondo contatore che desideri tracciare. Per questo esempio, selezionare *IOPS - Totale*.

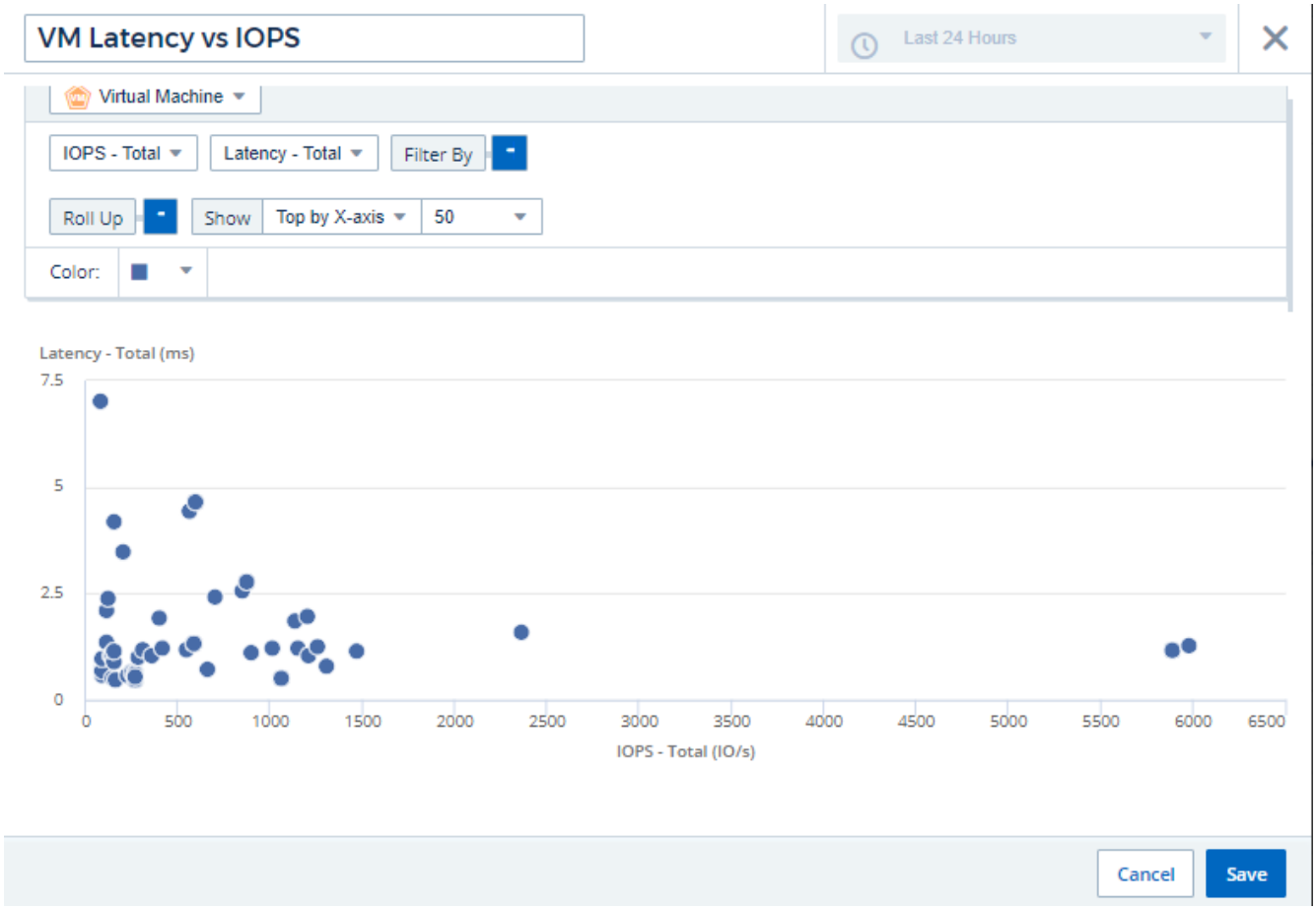
   IOPS - Totale è rappresentato lungo l'asse Y nel grafico. Le VM con latenza più elevata vengono visualizzate sul lato destro del grafico. Vengono visualizzate solo le 100 VM con la latenza più elevata, perché l'impostazione corrente è **In alto per asse X**.



5. Ora invertiamo l'ordine dei contatori impostando il primo contatore su *IOPS - Totale* e il secondo su *Latenza - Totale*.

   Latenza - Totale è ora rappresentato lungo l'asse Y del grafico, mentre *IOPS - Totale* lungo l'asse X. Le VM con IOPS più elevati ora vengono visualizzate sul lato destro del grafico.

   Si noti che, poiché non abbiamo modificato l'impostazione **In alto sull'asse X**, il widget ora visualizza le prime 100 VM con IOPS più elevati, poiché questo è ciò che viene attualmente tracciato lungo l'asse X.



È possibile scegliere di visualizzare nel grafico i primi N tramite l'asse X, i primi N tramite l'asse Y, i secondi N tramite l'asse X o i secondi N tramite l'asse Y. Nel nostro ultimo esempio, il grafico mostra le prime 100 VM con il numero totale di IOPS più elevato. Se lo modifichiamo in **In alto per asse Y**, il grafico visualizzerà nuovamente le prime 100 VM con la latenza totale più elevata.

Tieni presente che in un grafico a dispersione puoi fare clic su un punto per visualizzare in dettaglio la pagina delle risorse per quella risorsa.

Dashboard di esempio

Esempio di dashboard: prestazioni della macchina virtuale

Oggigiorno le operazioni IT devono affrontare numerose sfide. Agli amministratori viene chiesto di fare di più con meno e avere una visibilità completa sui propri data center dinamici è fondamentale. In questo esempio, ti mostreremo come creare una dashboard con widget che ti forniscono informazioni operative sulle prestazioni della macchina virtuale (VM) sul tuo tenant. Seguendo questo esempio e creando widget adatti alle tue esigenze specifiche, puoi fare cose come visualizzare le prestazioni dello storage backend rispetto alle prestazioni della macchina virtuale frontend oppure visualizzare la latenza della VM rispetto alla richiesta di I/O.

Informazioni su questo compito

Qui creeremo una dashboard delle prestazioni della macchina virtuale contenente quanto segue:

- una tabella che elenca i nomi delle VM e i dati sulle prestazioni
- un grafico che confronta la latenza della VM con la latenza dello storage
- un grafico che mostra lettura, scrittura e IOPS totali per le VM
- un grafico che mostra la velocità effettiva massima per le tue VM

Questo è solo un esempio basilare. Puoi personalizzare la tua dashboard per evidenziare e confrontare i dati sulle prestazioni che preferisci, in modo da individuare le migliori pratiche operative.

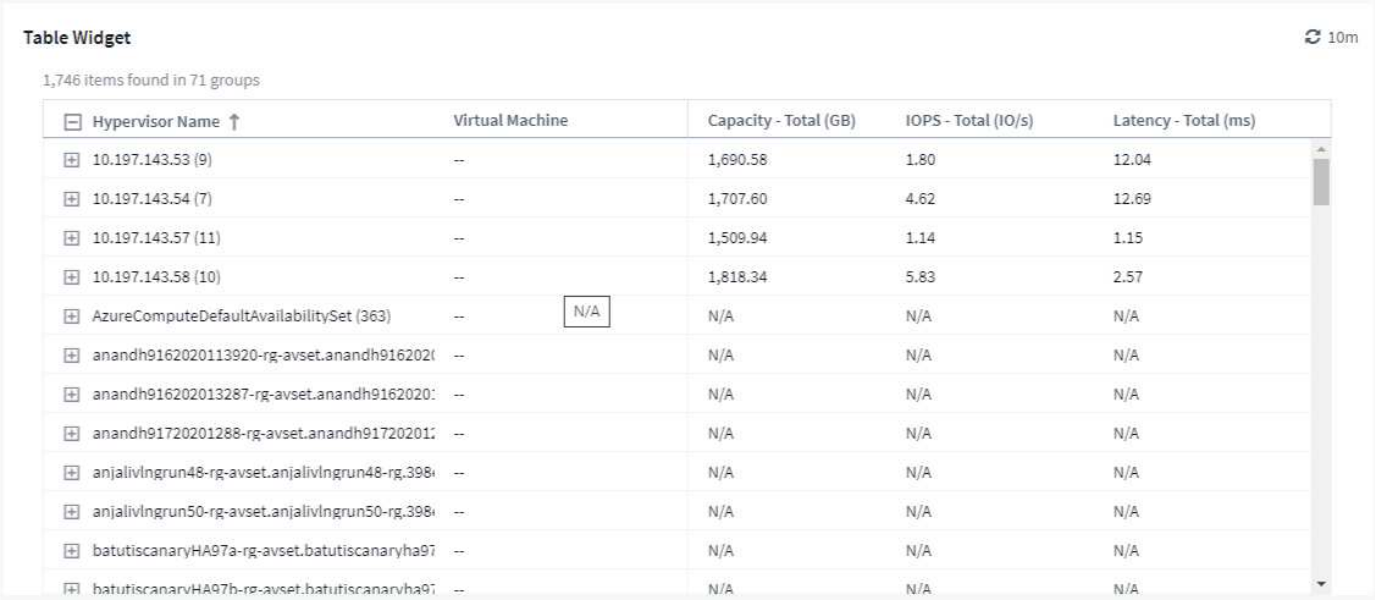
Passi

1. Accedi a Insight come utente con autorizzazioni amministrative.
2. Dal menu **Dashboard**, seleziona **[+Nuova dashboard]**.

   Si apre la pagina **Nuova dashboard**.

3. Nella parte superiore della pagina, inserisci un nome univoco per la dashboard, ad esempio "Prestazioni VM per applicazione".
4. Fare clic su **Salva** per salvare la dashboard con il nuovo nome.
5. Cominciamo ad aggiungere i nostri widget. Se necessario, fare clic sull'icona **Modifica** per abilitare la modalità di modifica.
6. Fare clic sull'icona **Aggiungi widget** e selezionare **Tabella** per aggiungere un nuovo widget tabella alla dashboard.

   Si apre la finestra di dialogo Modifica widget. I dati predefiniti visualizzati riguardano tutti gli archivi del tuo tenant.



1. Possiamo personalizzare questo widget. Nel campo Nome in alto, elimina "Widget 1" e inserisci "Tabella delle prestazioni della macchina virtuale".
2. Fare clic sul menu a discesa del tipo di risorsa e modificare *Archiviazione* in *Macchina virtuale*.

   I dati della tabella cambiano per mostrare tutte le macchine virtuali nel tuo tenant.

3. Aggiungiamo alcune colonne alla tabella. Fare clic sull'icona dell'ingranaggio a destra e selezionare *Nome*

hypervisor, *IOPS - Totale* e *Latenza - Totale*. Puoi anche provare a digitare il nome nella ricerca per visualizzare rapidamente il campo desiderato.

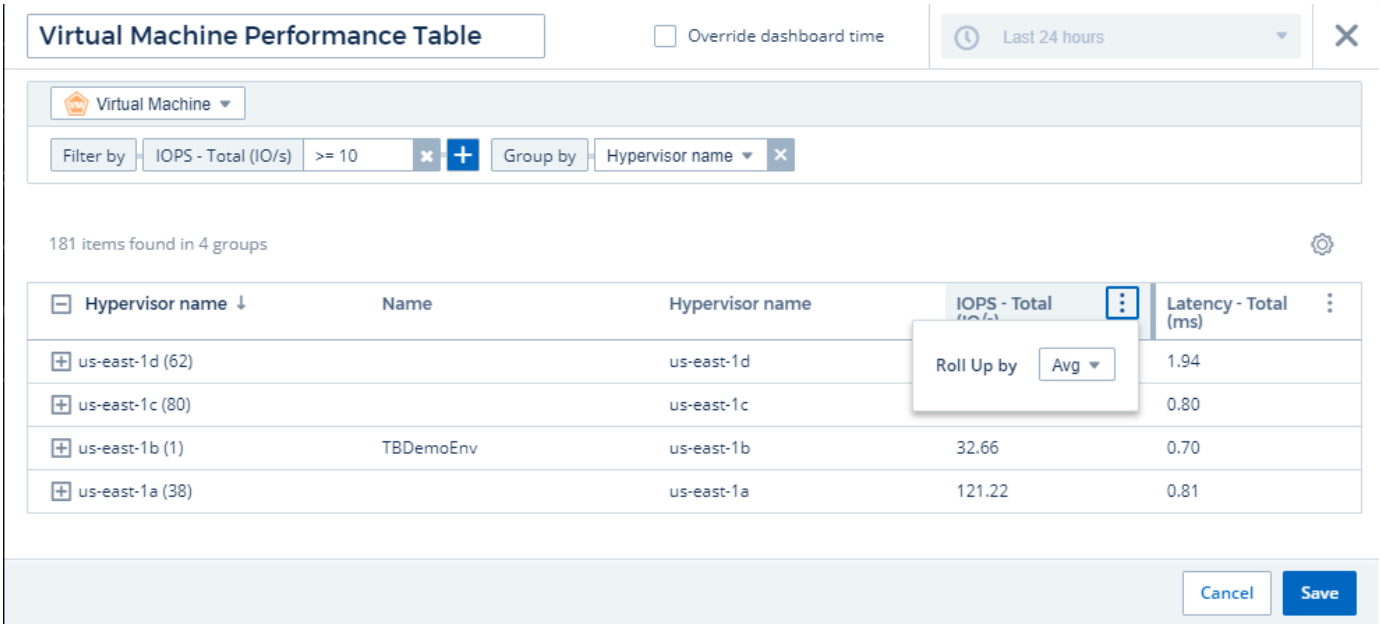
Queste colonne vengono ora visualizzate nella tabella. È possibile ordinare la tabella in base a una qualsiasi di queste colonne. Si noti che le colonne vengono visualizzate nell'ordine in cui sono state aggiunte al widget.

4. Per questo esercizio escluderemo le VM che non sono attivamente in uso, quindi filtriamo tutto ciò che ha meno di 10 IOPS totali. Fare clic sul pulsante **[+]** accanto a **Filtra per** e selezionare *IOPS - Totale*. Fare clic su **Qualsiasi** e immettere "10" nel campo **da**. Lasciare vuoto il campo **a**. Fare clic all'esterno del campo filtro o premere Invio per impostare il filtro.

   Nella tabella vengono ora visualizzate solo le VM con 10 o più IOPS totali.

5. Possiamo ulteriormente comprimere la tabella raggruppando i risultati. Fare clic sul pulsante **[+]** accanto a **Raggruppa per** e selezionare un campo in base al quale raggruppare, ad esempio *Applicazione* o *Nome hypervisor*. Il raggruppamento viene applicato automaticamente.

   Le righe della tabella sono ora raggruppate in base alle impostazioni. È possibile espandere e comprimere i gruppi in base alle proprie esigenze. Le righe raggruppate mostrano i dati raggruppati per ciascuna colonna. Alcune colonne consentono di scegliere il metodo di rollup per quella colonna.



1. Dopo aver personalizzato il widget della tabella in base alle tue esigenze, clicca sul pulsante **[Salva]**.

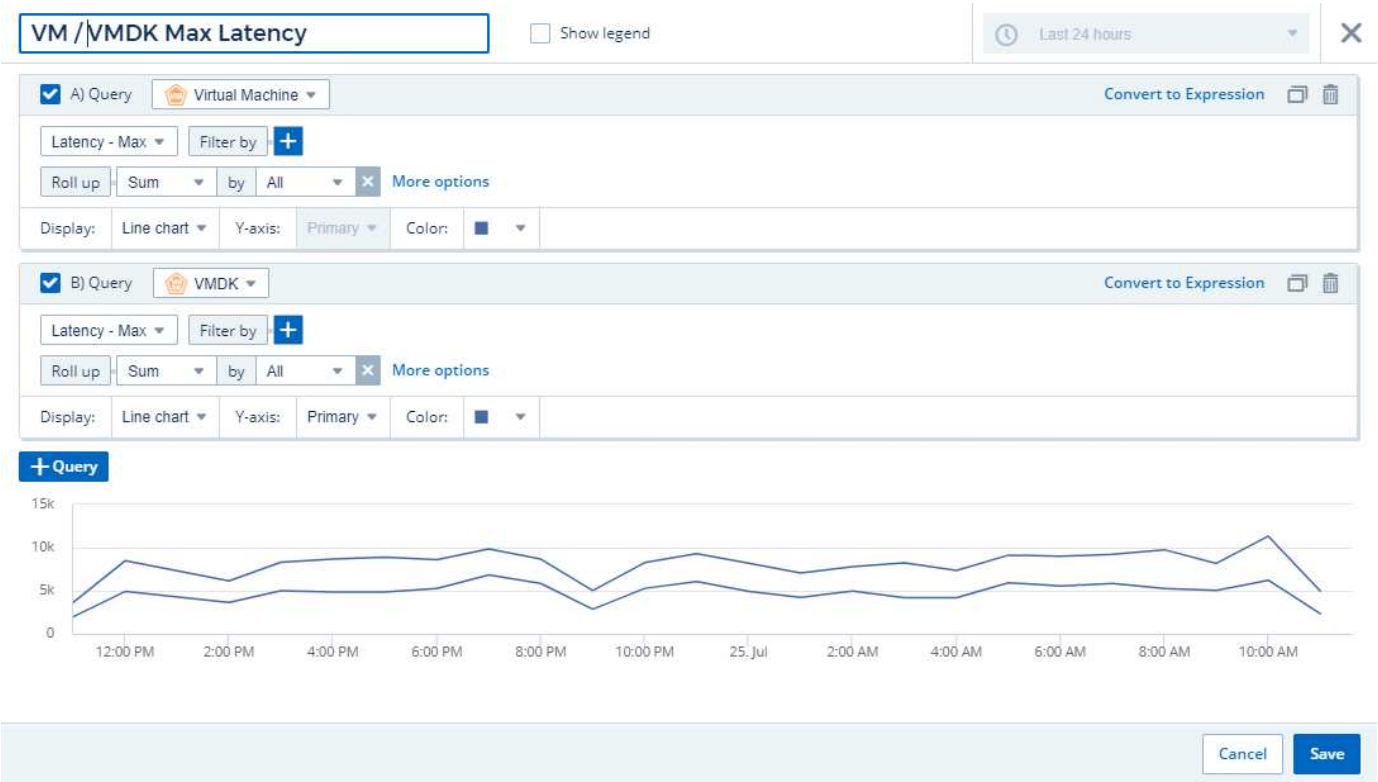
   Il widget della tabella viene salvato nella dashboard.

È possibile ridimensionare il widget sulla dashboard trascinandone l'angolo inferiore destro. Allarga il widget per mostrare chiaramente tutte le colonne. Fare clic su **Salva** per salvare la dashboard corrente.

Successivamente aggiungeremo alcuni grafici per mostrare le prestazioni della nostra VM. Creiamo un grafico a linee che confronta la latenza della VM con la latenza del VMDK.

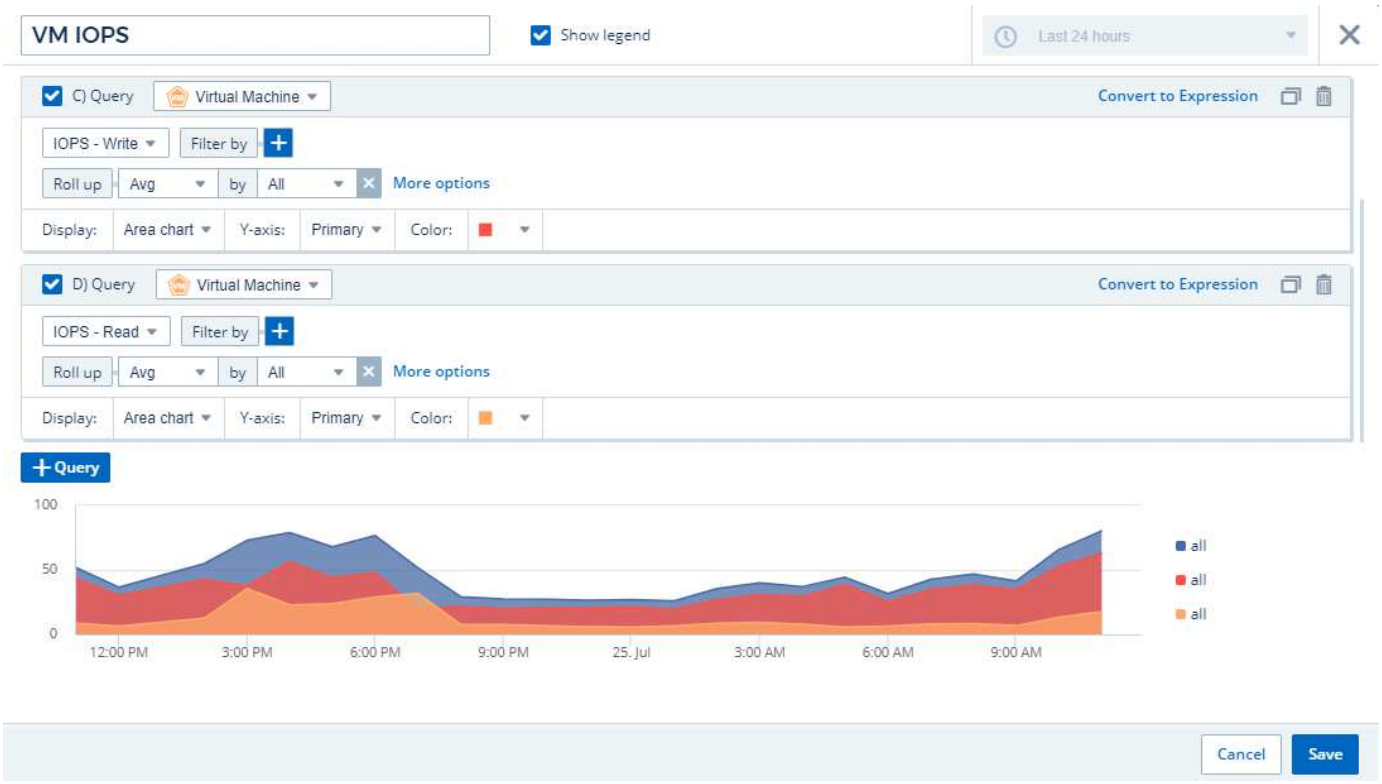
1. Se necessario, fare clic sull'icona **Modifica** nella dashboard per abilitare la modalità di modifica.
2. Fare clic sull'icona **[Aggiungi widget]** e selezionare *Grafico a linee* per aggiungere un nuovo widget grafico a linee alla dashboard.

3. Si apre la finestra di dialogo **Modifica widget**. Assegna a questo widget il nome "VM/VMDK Massima latenza"
4. Selezionare **Macchina virtuale** e scegliere *Latenza - Max*. Imposta i filtri che preferisci oppure lascia vuoto il campo **Filtra per**. Per **Arrotonda**, seleziona *Somma* per *Tutti*. Visualizza questi dati come un *grafico a linee* e lascia *asse Y* come *primario*.
5. Fare clic sul pulsante **[+Query]** per aggiungere una seconda riga di dati. Per questa riga, selezionare *VMDK* e *Latenza - Max*. Imposta i filtri che preferisci oppure lascia vuoto il campo **Filtra per**. Per **Arrotonda**, seleziona *Somma* per *Tutti*. Visualizza questi dati come un *grafico a linee* e lascia *asse Y* come *primario*.
6. Fare clic su **[Salva]** per aggiungere questo widget alla dashboard.



Successivamente aggiungeremo un grafico che mostra la lettura, la scrittura e gli IOPS totali della VM in un unico grafico.

1. Fare clic sull'icona **[Aggiungi widget]** e selezionare *Grafico ad area* per aggiungere un nuovo widget grafico ad area alla dashboard.
2. Si apre la finestra di dialogo Modifica widget. Assegna a questo widget il nome "VM IOPS"
3. Selezionare **Macchina virtuale** e scegliere *IOPS - Totale*. Imposta i filtri che desideri oppure lascia vuoto **Filtra per**. Per **Arrotonda**, scegli *Somma* per *Tutti*. Visualizza questi dati come un *Grafico ad area* e lascia *Asse Y* come *Principale*.
4. Fare clic sul pulsante **[+Query]** per aggiungere una seconda riga di dati. Per questa riga, seleziona **Macchina virtuale** e scegli *IOPS - Lettura*.
5. Fare clic sul pulsante **[+Query]** per aggiungere una terza riga di dati. Per questa riga, seleziona **Macchina virtuale** e scegli *IOPS - Scrittura*.
6. Fare clic su **Mostra legenda** per visualizzare una legenda per questo widget sulla dashboard.



1. Fare clic su **[Salva]** per aggiungere questo widget alla dashboard.

Successivamente aggiungeremo un grafico che mostra la produttività della VM per ciascuna applicazione associata alla VM. Per questo utilizzeremo la funzione Roll Up.

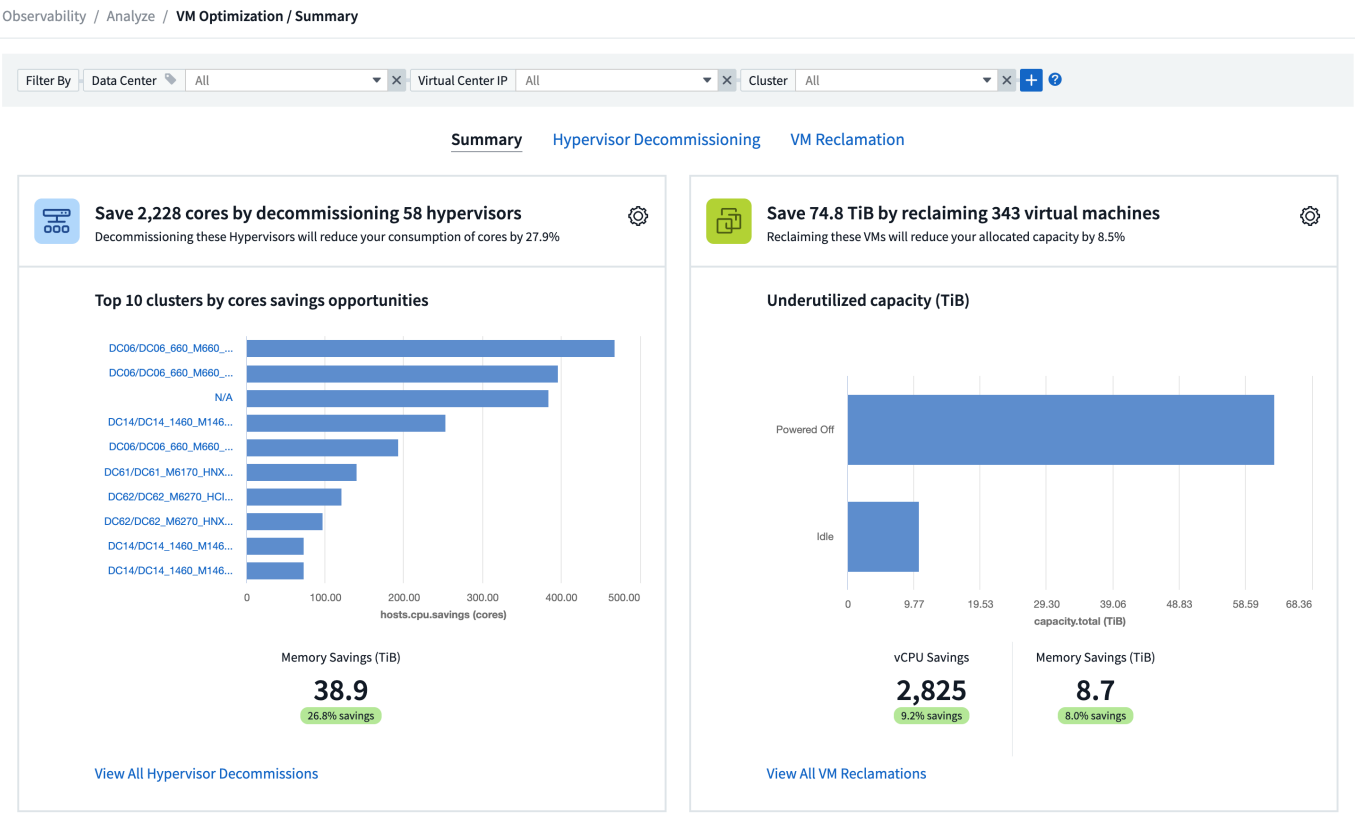
1. Fare clic sull'icona **[Aggiungi widget]** e selezionare *Grafico a linee* per aggiungere un nuovo widget grafico a linee alla dashboard.
2. Si apre la finestra di dialogo Modifica widget. Assegna a questo widget il nome "Rendimento VM per applicazione"
3. Selezionare Macchina virtuale e scegliere Throughput - Totale. Imposta i filtri che preferisci oppure lascia vuoto il campo Filtra per. Per Roll up, seleziona "Max" e seleziona "Applicazione" o "Nome". Mostra le 10 applicazioni più popolari. Visualizza questi dati come grafico a linee e lascia l'asse Y come asse primario.
4. Fare clic su **[Salva]** per aggiungere questo widget alla dashboard.

È possibile spostare i widget sulla dashboard tenendo premuto il pulsante del mouse in un punto qualsiasi della parte superiore del widget e trascinandolo in una nuova posizione.

È possibile ridimensionare i widget trascinando l'angolo inferiore destro.

Dopo aver apportato le modifiche, assicurati di **[Salvare]** la dashboard.

La dashboard finale delle prestazioni della VM avrà un aspetto simile a questo:



Lavorare con le query

Interrogazione di asset e metriche

Interroga le risorse fisiche e virtuali della tua infrastruttura per monitorare le prestazioni, risolvere i problemi ed eseguire ricerche granulari basate su criteri personalizzati come le annotazioni. Data Infrastructure Insights consente di eseguire query su diverse tipologie di risorse—dagli array di storage e host alle applicazioni e alle macchine virtuali—insieme a metriche di integrazione da Kubernetes, Docker e ONTAP Advanced Data per una visibilità completa.

Si noti che le regole di annotazione, che assegnano automaticamente annotazioni alle risorse, richiedono una query che è stata condivisa con tutti. Vedere di seguito per ulteriori informazioni sulla condivisione delle query.

È possibile interrogare le risorse di inventario fisiche o virtuali (e le relative metriche) sul tenant oppure le metriche fornite con l'integrazione, ad esempio Kubernetes o ONTAP Advanced Data.

Attività di inventario

Tutti i tipi di asset di inventario (chiamati anche infrastruttura) (storage, switch, VM, Application, ecc.) possono essere utilizzati in query, widget della dashboard e pagine di destinazione degli asset personalizzate. I campi e i contatori disponibili per filtri, espressioni e visualizzazione varieranno tra i tipi di asset.

Metriche di integrazione

Oltre a eseguire query sulle risorse di inventario e sulle relative metriche di prestazioni, è possibile eseguire query anche sulle metriche dei **dati di integrazione**, come quelle generate da Kubernetes o Docker, o fornite

con ONTAP Advanced Metrics.

Condivisione delle query

Controlla l'accesso alle tue query scegliendo chi può visualizzarle e modificarle. Per impostazione predefinita, le nuove query sono private e visibili solo a te e puoi scegliere di condividerle con utenti specifici o con l'intera organizzazione con livelli di autorizzazione flessibili (Sola lettura o Modifica).

Puoi scegliere di condividere la query con Everyone o con utenti selezionati, con autorizzazioni di modifica o di sola lettura.

Gli utenti con autorizzazione Account Owner possono visualizzare tutte le query, indipendentemente dall'impostazione della privacy.

Creazione di query

Le query consentono di cercare le risorse del tenant a livello granulare, consentendo di filtrare i dati desiderati e ordinare i risultati a proprio piacimento.

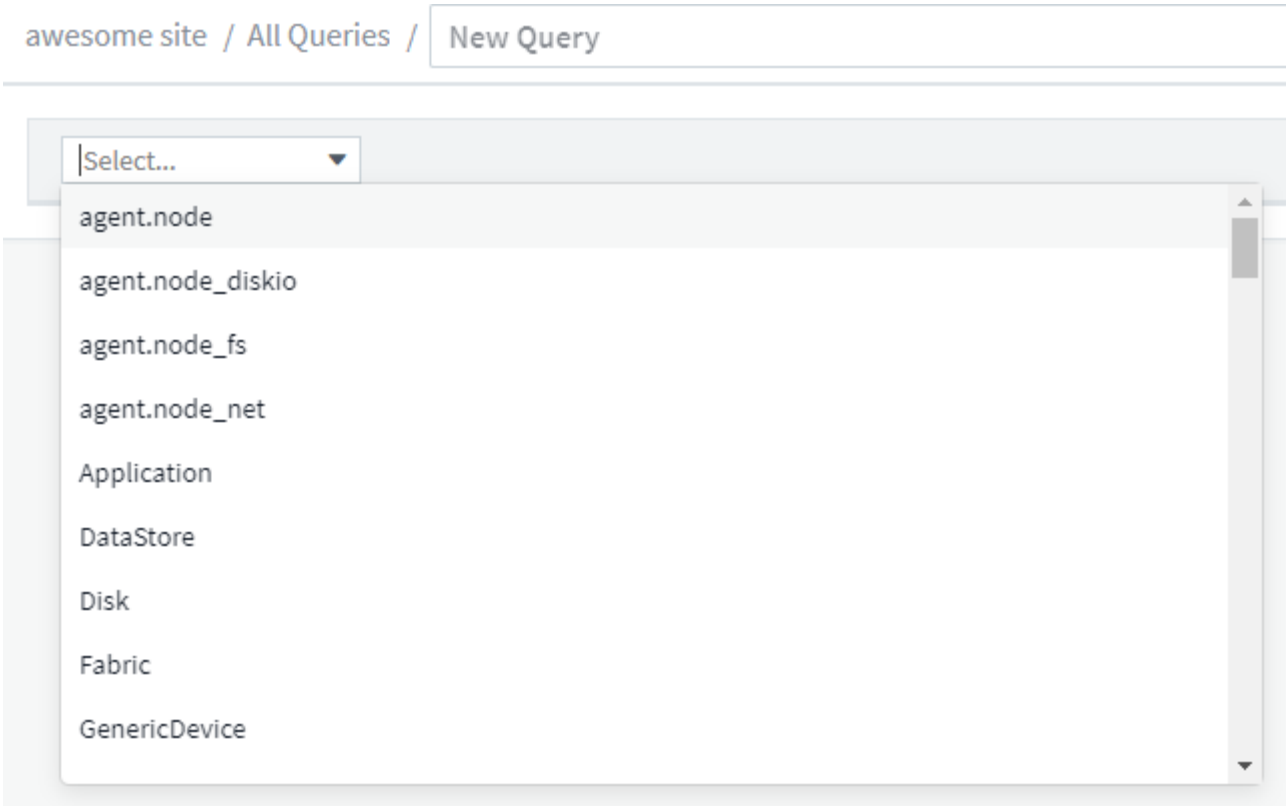
Ad esempio, è possibile creare una query per *volumi*, aggiungere un filtro per trovare specifici *archiviazioni* associati ai volumi selezionati, aggiungere un altro filtro per trovare una specifica *annotazione* come "Livello 1" sulle archiviazioni selezionate e infine aggiungere un altro filtro per trovare tutte le archiviazioni con *IOPS - Lettura (IO/s)* maggiore di 25. Una volta visualizzati i risultati, è possibile ordinare le colonne di informazioni associate alla query in ordine crescente o decrescente.

Nota: quando viene aggiunto un nuovo raccoglitore di dati che acquisisce risorse o vengono effettuate assegnazioni di annotazioni o applicazioni, è possibile eseguire query su tali nuove risorse, annotazioni o applicazioni solo dopo che le query sono state indicizzate. L'indicizzazione avviene a intervalli regolari programmati o durante determinati eventi, ad esempio l'esecuzione di regole di annotazione.

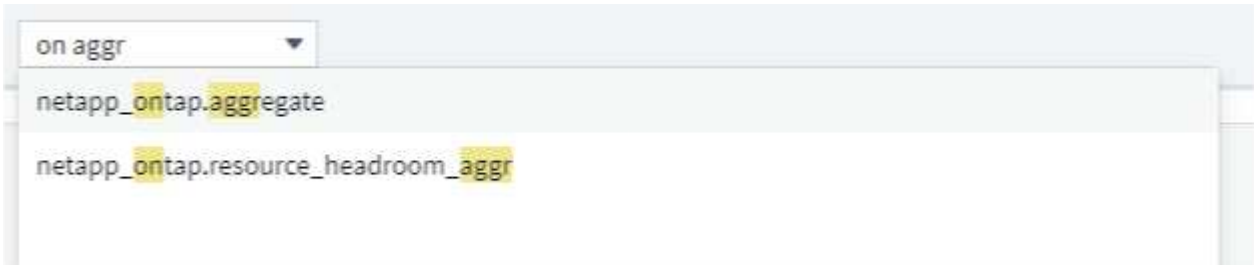
Creare una query è molto semplice:

1. Vai a **Query > *+Nuova query**.
2. Dall'elenco "Seleziona…", seleziona il tipo di oggetto per il quale desideri effettuare la query. Puoi scorrere l'elenco oppure iniziare a digitare per trovare più rapidamente ciò che stai cercando.

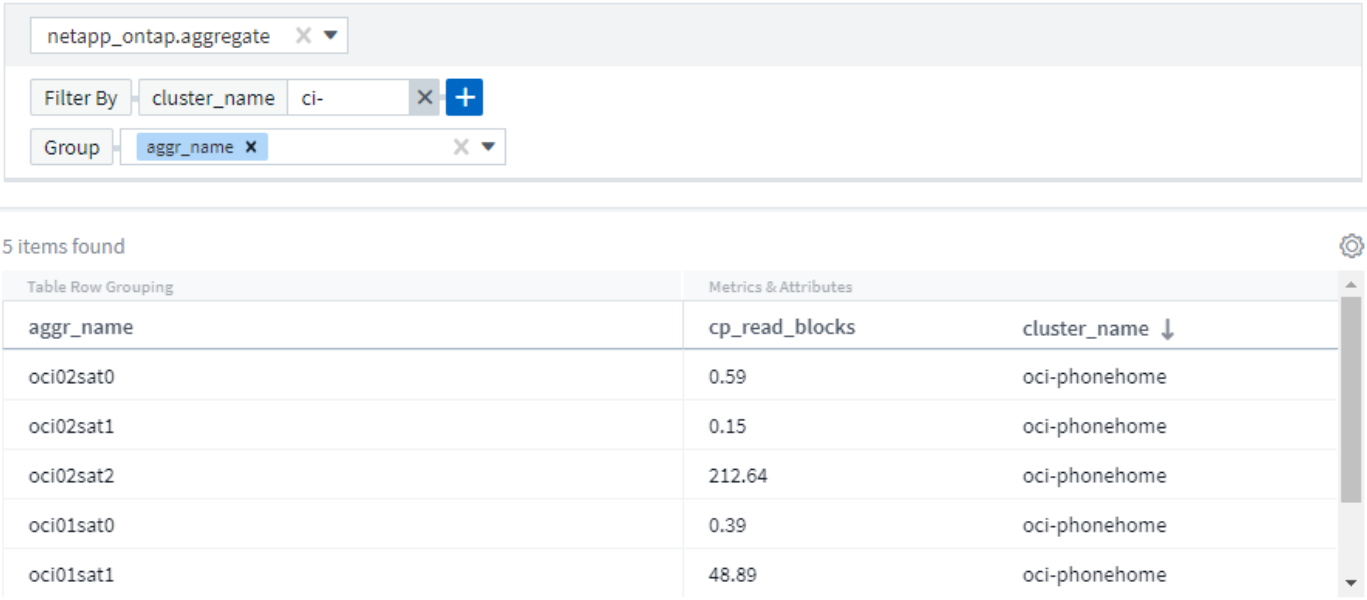
Elenco di scorrimento:



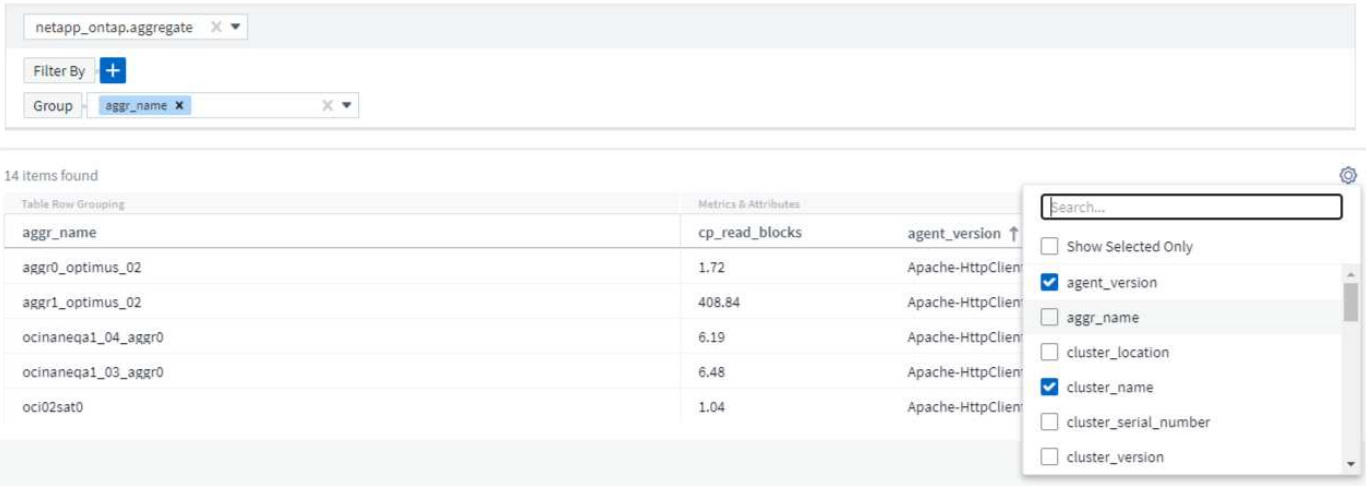
Digita per cercare:



Puoi aggiungere filtri per restringere ulteriormente la tua query cliccando sul pulsante **+** nel campo **Filtra per**. Raggruppa le righe per oggetto o attributo. Quando si lavora con dati di integrazione (Kubernetes, ONTAP Advanced Metrics, ecc.), è possibile raggruppare in base a più attributi, se lo si desidera.



L'elenco dei risultati della query mostra un numero di colonne predefinite, a seconda del tipo di oggetto cercato. Per aggiungere, rimuovere o modificare le colonne, fare clic sull'icona dell'ingranaggio a destra della tabella. Le colonne disponibili variano in base al tipo di risorsa/metrica.



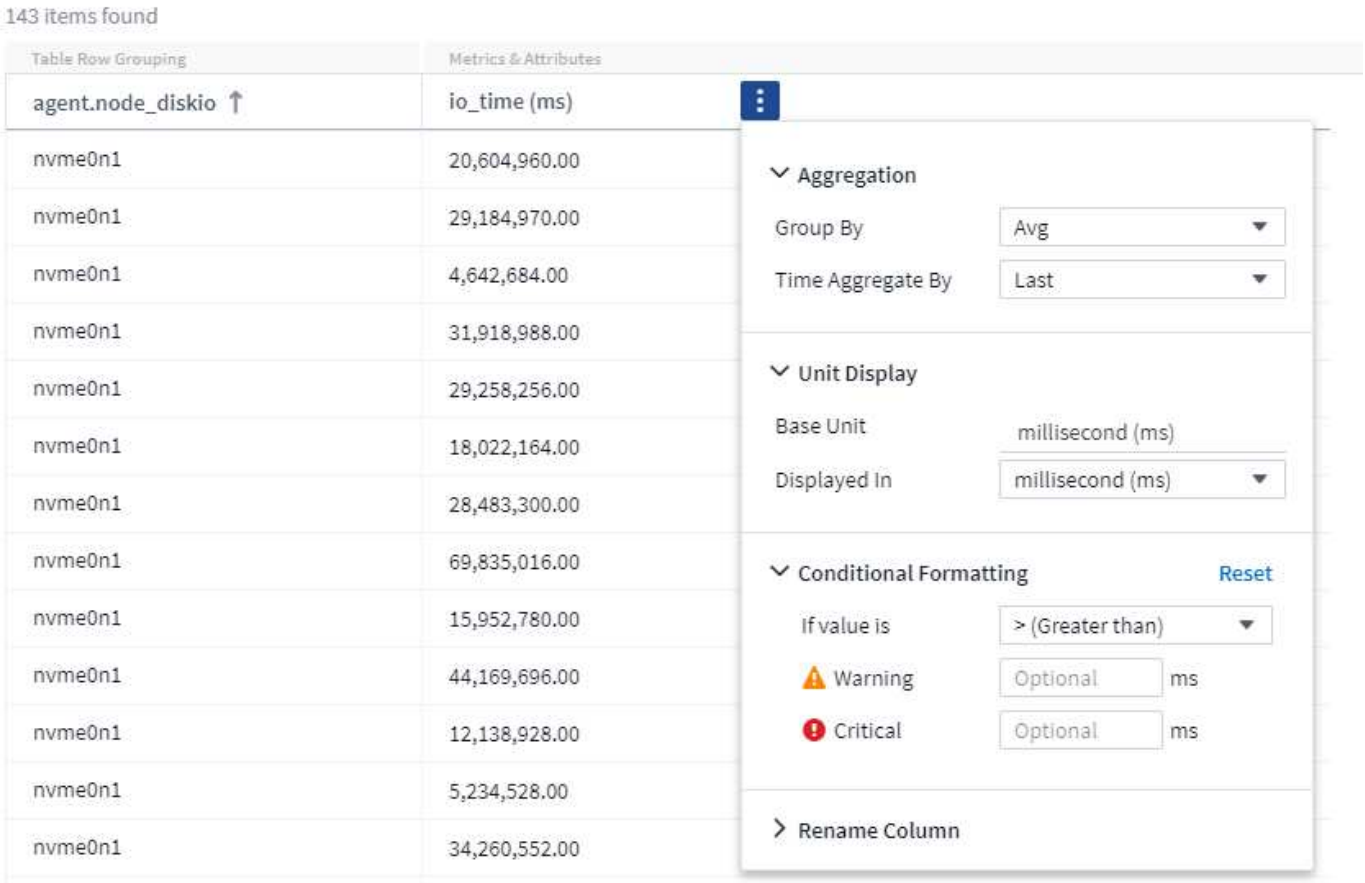
Guardalo in azione

"Esplora e analizza con le query in Data Infrastructure Insights (video)"

Scelta di aggregazione, unità, formattazione condizionale

Aggregazione e unità

Per le colonne "valore", è possibile perfezionare ulteriormente i risultati della query scegliendo il modo in cui vengono aggregati i valori visualizzati e selezionando le unità in cui tali valori vengono visualizzati. Per accedere a queste opzioni, selezionare il menu "tre punti" nell'angolo superiore di una colonna.



Unità

È possibile selezionare le unità in cui visualizzare i valori. Ad esempio, se la colonna selezionata mostra la capacità grezza e i valori sono mostrati in GiB, ma si preferisce visualizzarli in TiB, è sufficiente selezionare TiB dal menu a discesa Visualizzazione unità.

Aggregazione

Allo stesso modo, se i valori mostrati sono aggregati dai dati sottostanti come "Media", ma si preferisce mostrare la somma di tutti i valori, selezionare "Somma" dal menu a discesa *Raggruppa per* (se si desidera che i valori raggruppati mostrino le somme) o dal menu a discesa *Aggregazione temporale per* (se si desidera che i valori di riga mostrino le somme dei dati sottostanti).

È possibile scegliere di aggregare i punti dati raggruppati in base a *Media, Max, Min o Somma*.

È possibile aggregare i dati delle singole righe in base a *Media, Ultimo punto dati acquisito, Massimo, Minimo o Somma*.

Formattazione condizionale

La formattazione condizionale consente di evidenziare le soglie di livello di avviso e di livello critico nell'elenco dei risultati della query, offrendo visibilità immediata ai valori anomali e ai punti dati eccezionali.

La formattazione condizionale viene impostata separatamente per ogni colonna. Ad esempio, è possibile scegliere un set di soglie per una colonna di capacità e un altro set per una colonna di produttività.

Rinomina colonna

Rinominando una colonna si modifica il nome visualizzato nell'elenco dei risultati della query. Il nome della nuova colonna viene visualizzato anche nel file risultante se si esporta l'elenco delle query in formato .CSV.

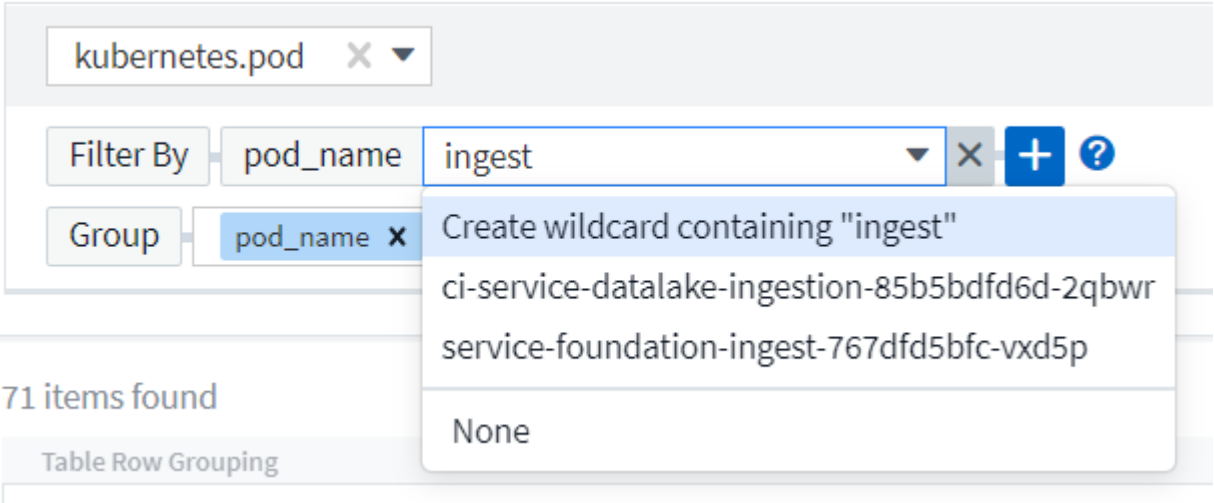
Salva

Dopo aver configurato la query in modo da visualizzare i risultati desiderati, puoi fare clic sul pulsante **Salva** per salvare la query per un utilizzo futuro. Dategli un nome significativo e unico.

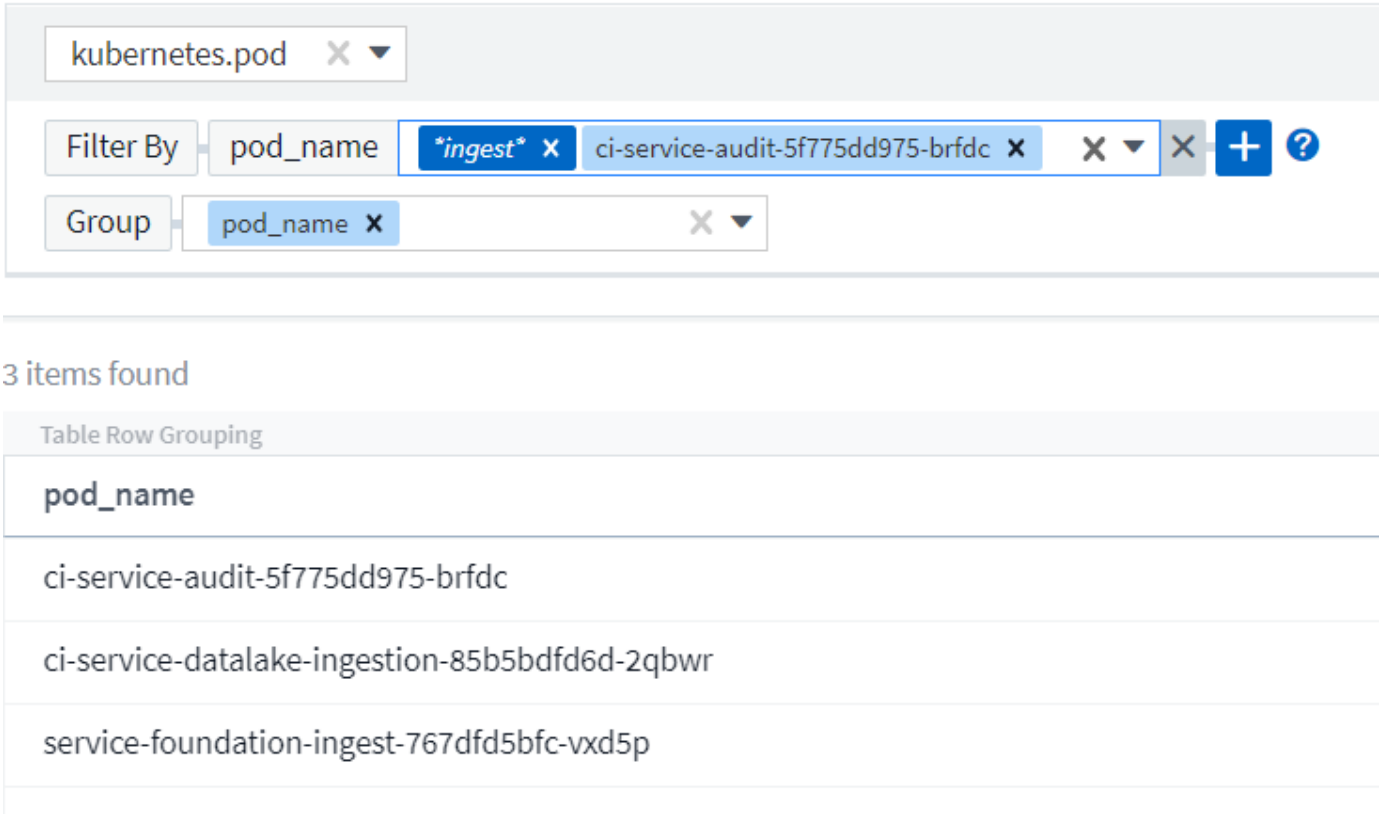
Ulteriori informazioni sul filtraggio

Caratteri jolly ed espressioni

Quando si filtrano valori di testo o di elenco in query o widget della dashboard, quando si inizia a digitare viene presentata l'opzione per creare un **filtro con caratteri jolly** in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione jolly. È anche possibile creare **espressioni** utilizzando NOT o OR, oppure selezionare l'opzione "Nessuno" per filtrare i valori nulli nel campo.



I filtri basati su caratteri jolly o espressioni (ad esempio NOT, OR, "Nessuno", ecc.) vengono visualizzati in blu scuro nel campo filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in azzurro.



Si noti che il filtro con caratteri jolly ed espressioni funziona con testo o elenchi, ma non con valori numerici, date o valori booleani.

Filtri di affinamento

Per affinare il filtro puoi usare quanto segue:

Filtro	Cosa fa	Esempio	Risultato
* (Asterisco)	ti permette di cercare tutto	vol*rhel	restituisce tutte le risorse che iniziano con "vol" e finiscono con "rhel"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	BOS-PRD??-S12	restituisce BOS-PRD***12*** -S12, BOS-PRD***23***-S12 e così via
O	consente di specificare più entità	FAS2240 O CX600 O FAS3270	restituisce uno qualsiasi tra FAS2440, CX600 o FAS3270
NON	consente di escludere il testo dai risultati della ricerca	NON EMC*	restituisce tutto ciò che non inizia con "EMC"
Nessuno	cerca valori NULL in tutti i campi	*Nessuno*	restituisce risultati in cui il campo di destinazione è vuoto

Non *	cerca valori NULL nei campi *solo testo*	Non *	restituisce risultati in cui il campo di destinazione è vuoto

Se si racchiude una stringa di filtro tra virgolette doppie, Insight considera tutto ciò che si trova tra la prima e l'ultima virgoletta come una corrispondenza esatta. Tutti i caratteri speciali o gli operatori all'interno delle virgolette verranno trattati come valori letterali. Ad esempio, filtrando per "*" si otterranno risultati che sono un asterisco letterale; in questo caso l'asterisco non verrà trattato come un carattere jolly. Anche gli operatori OR e NOT verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

Filtraggio per valori booleani

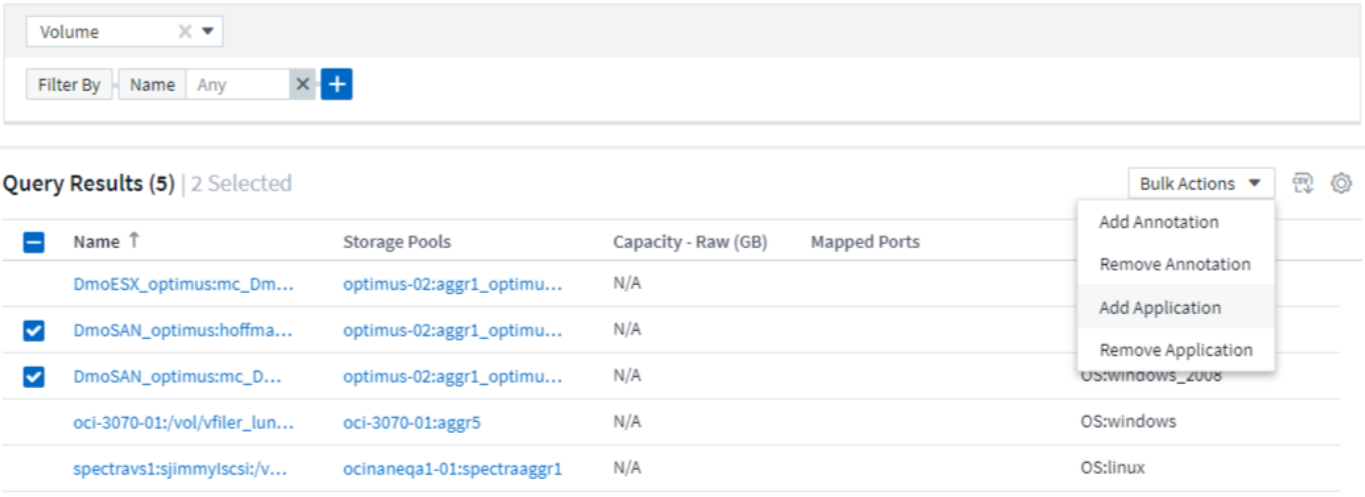
Quando si filtra un valore booleano, potrebbero essere presentate le seguenti opzioni di filtraggio:

- **Qualsiasi**: restituirà *tutti* i risultati, compresi i risultati impostati su "Sì", "No" o non impostati affatto.
- **Sì**: Restituisce solo risultati "Sì". Si noti che DII mostra "Sì" come segno di spunta nella maggior parte delle tabelle. I valori possono essere impostati su "True", "On", ecc.; DII li tratta tutti come "Sì".
- **No**: restituisce solo risultati "No". Si noti che DII mostra "No" come una "X" nella maggior parte delle tabelle. I valori possono essere impostati su "Falso", "Off", ecc.; DII li tratta tutti come "No".
- **Nessuno**: restituisce solo i risultati in cui il valore non è stato impostato. Chiamati anche valori "Null".

Cosa devo fare ora che ho i risultati della query?

Le query rappresentano un modo semplice per aggiungere annotazioni o assegnare applicazioni alle risorse. Tieni presente che puoi assegnare applicazioni o annotazioni solo alle risorse del tuo inventario (disco, archiviazione, ecc.). Le metriche di integrazione non possono accettare assegnazioni di annotazioni o applicazioni.

Per assegnare un'annotazione o un'applicazione alle risorse risultanti dalla query, seleziona semplicemente la/le risorsa/e utilizzando la colonna delle caselle di controllo a sinistra della tabella dei risultati, quindi fai clic sul pulsante **Azioni in blocco** a destra. Scegli l'azione desiderata da applicare alle risorse selezionate.



Le regole di annotazione richiedono una query

Se stai configurando"Regole di annotazione" , ogni regola deve avere una query sottostante con cui lavorare. Ma come hai visto sopra, le query possono essere ampie o ristrette, a seconda delle tue esigenze.

Visualizzazione delle query

Puoi visualizzare le tue query per monitorare le tue risorse e modificare il modo in cui le query visualizzano i dati relativi alle tue risorse.

Passi

1. Accedi al tuo tenant Data Infrastructure Insights .
2. Fare clic su **Query** e selezionare **Mostra tutte le query**. È possibile modificare la modalità di visualizzazione delle query eseguendo una delle seguenti operazioni:
3. È possibile immettere del testo nella casella filtro per cercare di visualizzare query specifiche.
4. È possibile modificare l'ordinamento delle colonne nella tabella delle query in crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell'intestazione della colonna.
5. Per ridimensionare una colonna, passa il mouse sull'intestazione della colonna finché non appare una barra blu. Posiziona il mouse sulla barra e trascinalo verso destra o verso sinistra.
6. Per spostare una colonna, fare clic sull'intestazione della colonna e trascinarla verso destra o verso sinistra.

Quando scorri i risultati della query, tieni presente che potrebbero cambiare poiché Data Infrastructure Insights interroga automaticamente i tuoi raccoglitori di dati. Ciò potrebbe comportare la mancanza di alcuni articoli o la loro visualizzazione fuori ordine, a seconda di come sono ordinati.

Esportazione dei risultati della query in un file .CSV

È possibile esportare i risultati di qualsiasi query in un file .CSV, che consentirà di analizzare i dati o di importarli in un'altra applicazione.

Passi

1. Accedi a Data Infrastructure Insights.
2. Fare clic su **Query** e selezionare **Mostra tutte le query**.

   Viene visualizzata la pagina Query.

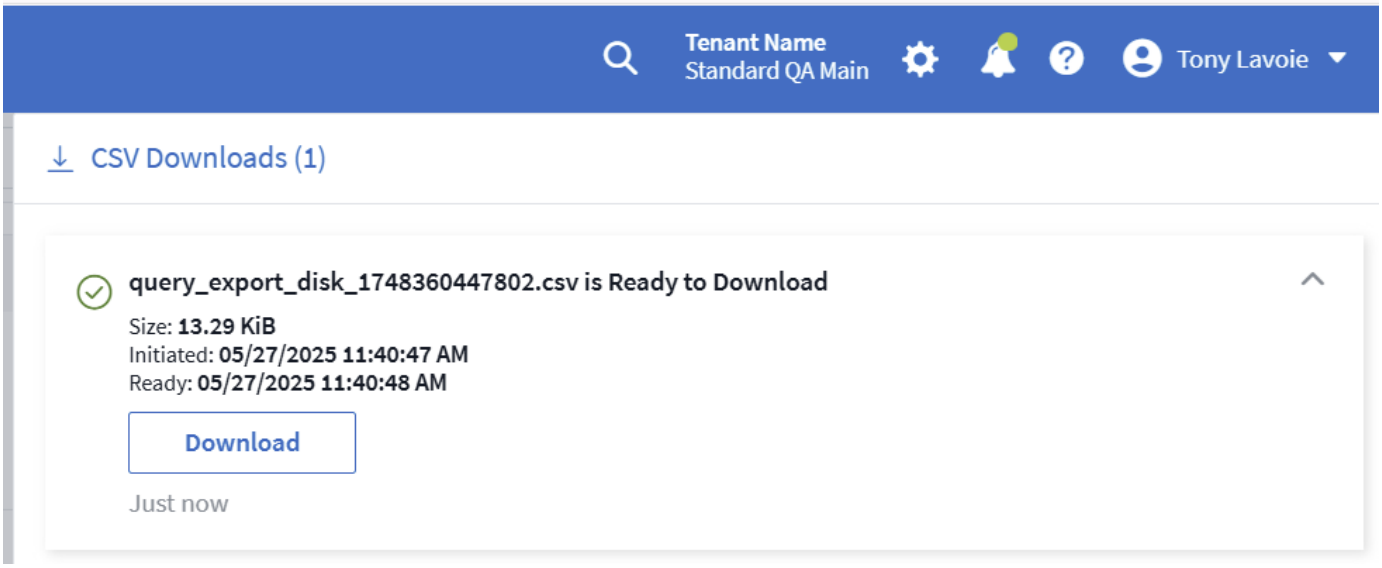
3. Fare clic su una query.
4. Clic per esportare i risultati della query in un file .CSV.

> L'esportazione in formato .CSV è disponibile anche nel menu "tre punti" nei widget delle tabelle della dashboard e nella maggior parte delle tabelle delle landing page.

Esportazione asincrona

L'esportazione dei dati in formato .CSV può richiedere da pochi secondi a diverse ore, a seconda della quantità di dati da esportare. Data Infrastructure Insights esporta tali dati in modo asincrono, così puoi continuare a lavorare mentre il file .CSV viene compilato.

Visualizza e scarica le tue esportazioni .CSV selezionando l'icona "Campana" nella barra degli strumenti in alto a destra.



I dati esportati rifletteranno il filtro corrente, le colonne e i nomi delle colonne visualizzati.

Virgole nei nomi delle risorse

Nota: quando nel nome di una risorsa è presente una virgola, l'esportazione racchiude il nome tra virgolette, preservando il nome della risorsa e il formato .csv corretto.

Formato dell'ora o non formato dell'ora?

Quando si apre un file .CSV esportato con Excel, se si ha un nome di oggetto o un altro campo nel formato NN:NN (due cifre seguite da due punti seguiti da altre due cifre), Excel a volte interpreterà quel nome come un formato Ora, anziché come un formato Testo. Ciò può comportare la visualizzazione di valori errati in tali colonne da parte di Excel. Ad esempio, un oggetto denominato "81:45" verrebbe visualizzato in Excel come "81:45:00".

Per ovviare a questo problema, importa il file .CSV in Excel seguendo i passaggi seguenti:

1. Apri un nuovo foglio in Excel.
2. Nella scheda "Dati", seleziona "Da testo".
3. Individua il file .CSV desiderato e fai clic su "Importa".
4. Nella procedura guidata di importazione, seleziona "Delimitato" e fai clic su Avanti.
5. Selezionare "Virgola" come delimitatore e fare clic su Avanti.
6. Selezionare le colonne desiderate e scegliere "Testo" come formato dei dati della colonna.
7. Fare clic su Fine.

   Gli oggetti dovrebbero essere visualizzati in Excel nel formato corretto.

Modifica o eliminazione di una query

È possibile modificare i criteri associati a una query quando si desidera modificare i criteri di ricerca per le risorse su cui si sta eseguendo la query.

Modifica di una query

Passi

1. Fare clic su **Esplora** e selezionare **Tutte le query metriche**.

   Viene visualizzata la pagina Query.

2. Fare clic sul nome della query
3. Per aggiungere un criterio alla query, fare clic sull'icona Colonne e selezionare una metrica o un attributo dall'elenco.

Dopo aver apportato tutte le modifiche necessarie, procedere in uno dei seguenti modi:

- Fare clic sul pulsante **Salva** per salvare la query con il nome utilizzato inizialmente.
- Fare clic sul menu a discesa accanto al pulsante **Salva** e selezionare **Salva con nome** per salvare la query con un altro nome. Ciò non sovrascrive la query originale.
- Fare clic sul menu a discesa accanto al pulsante **Salva** e selezionare **Rinomina** per modificare il nome della query utilizzato inizialmente. Ciò sovrascrive la query originale.
- Fare clic sul menu a discesa accanto al pulsante **Salva** e selezionare **Ignora modifiche** per ripristinare la query alle ultime modifiche salvate.

Eliminazione di una query

Per eliminare una query, fare clic su **Query** e selezionare **Mostra tutte le query**, quindi eseguire una delle seguenti operazioni:

1. Fare clic sul menu "tre punti" a destra della query e fare clic su **Elimina**.
2. Fare clic sul nome della query e selezionare **Elimina** dal menu a discesa **Salva**.

Assegnazione di più applicazioni o rimozione di più applicazioni dalle risorse

È possibile assegnare più"applicazioni" aggiungere o rimuovere più applicazioni dalle risorse utilizzando una query anziché doverle assegnare o rimuovere manualmente.

Puoi usare questi passaggi per aggiungere o rimuovere"annotazioni" allo stesso modo.

Prima di iniziare

Devi aver già creato una query che trovi tutte le risorse che vuoi modificare.

Passi

1. Fare clic su **Esplora** e selezionare **Query metriche**.

   Viene visualizzata la pagina Query.

2. Fare clic sul nome della query che trova le risorse.

   Viene visualizzato l'elenco delle risorse associate alla query.

3. Selezionare le risorse desiderate nell'elenco oppure fare clic sulla casella di controllo in alto per selezionare Tutto.

Viene visualizzato il menu a discesa Azioni in blocco.

4. Per aggiungere un'applicazione alle risorse selezionate, fare clic su Azioni in blocco e selezionare **Aggiungi applicazione**.
5. Selezionare una o più applicazioni.

   È possibile selezionare più applicazioni per host, volumi interni, qtree e macchine virtuali; tuttavia, è possibile selezionare una sola applicazione per un volume o una condivisione.

6. Fare clic su **Salva**.
7. Per rimuovere un'applicazione assegnata alle risorse, fare clic su Azioni in blocco e selezionare **Rimuovi applicazione**.
8. Seleziona l'applicazione o le applicazioni che desideri rimuovere.
9. Fare clic su **Elimina**.

Tutte le nuove applicazioni assegnate sovrascrivono tutte le applicazioni sulla risorsa derivate da un'altra risorsa. Ad esempio, i volumi ereditano le applicazioni dagli host e quando a un volume vengono assegnate nuove applicazioni, la nuova applicazione ha la precedenza sull'applicazione derivata.

Dopo aver fatto clic su *Salva* per un'aggiunta in blocco o su *Rimuovi* per un'eliminazione in blocco, Data Infrastructure Insights ti informa che l'azione richiederà del tempo. Puoi ignorare questo messaggio; l'azione continuerà in background.

Per ambienti con grandi quantità di risorse correlate, l'ereditarietà delle assegnazioni delle applicazioni a tali risorse potrebbe richiedere diversi minuti. Se si hanno molti beni correlati, si prega di attendere più tempo affinché l'eredità avvenga.

Copia dei valori della tabella

È possibile copiare i valori delle tabelle negli appunti per utilizzarli nelle caselle di ricerca o in altre applicazioni.

Informazioni su questo compito

Esistono due metodi per copiare i valori dalle tabelle o i risultati delle query negli appunti.

Passi

1. Metodo 1: evidenziare il testo desiderato con il mouse, copiarlo e incollarlo nei campi di ricerca o in altre applicazioni.
2. Metodo 2: per i campi a valore singolo, passa il mouse sopra il campo e fai clic sull'icona degli appunti che appare. Il valore viene copiato negli appunti per essere utilizzato nei campi di ricerca o in altre applicazioni.

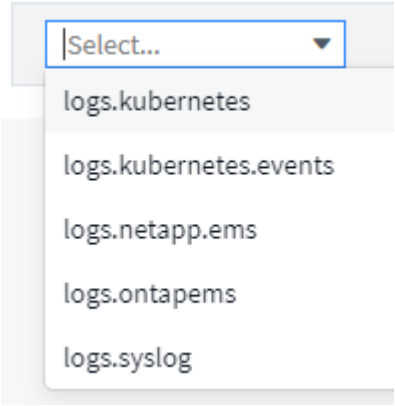
   Si noti che con questo metodo è possibile copiare solo i valori che sono collegamenti ad asset. Solo i campi che includono valori singoli (ad esempio quelli non elencati) hanno l'icona di copia.

Esploratore di log

Data Infrastructure Insights Log Explorer è un potente strumento per interrogare i log di sistema. Oltre ad agevolare le indagini, è anche possibile salvare una query di registro in un Monitor per ricevere avvisi quando vengono attivati specifici trigger di registro.

Per iniziare a esplorare i log, fare clic su **Query log > +Nuova query log**.

Selezionare un registro disponibile dall'elenco.

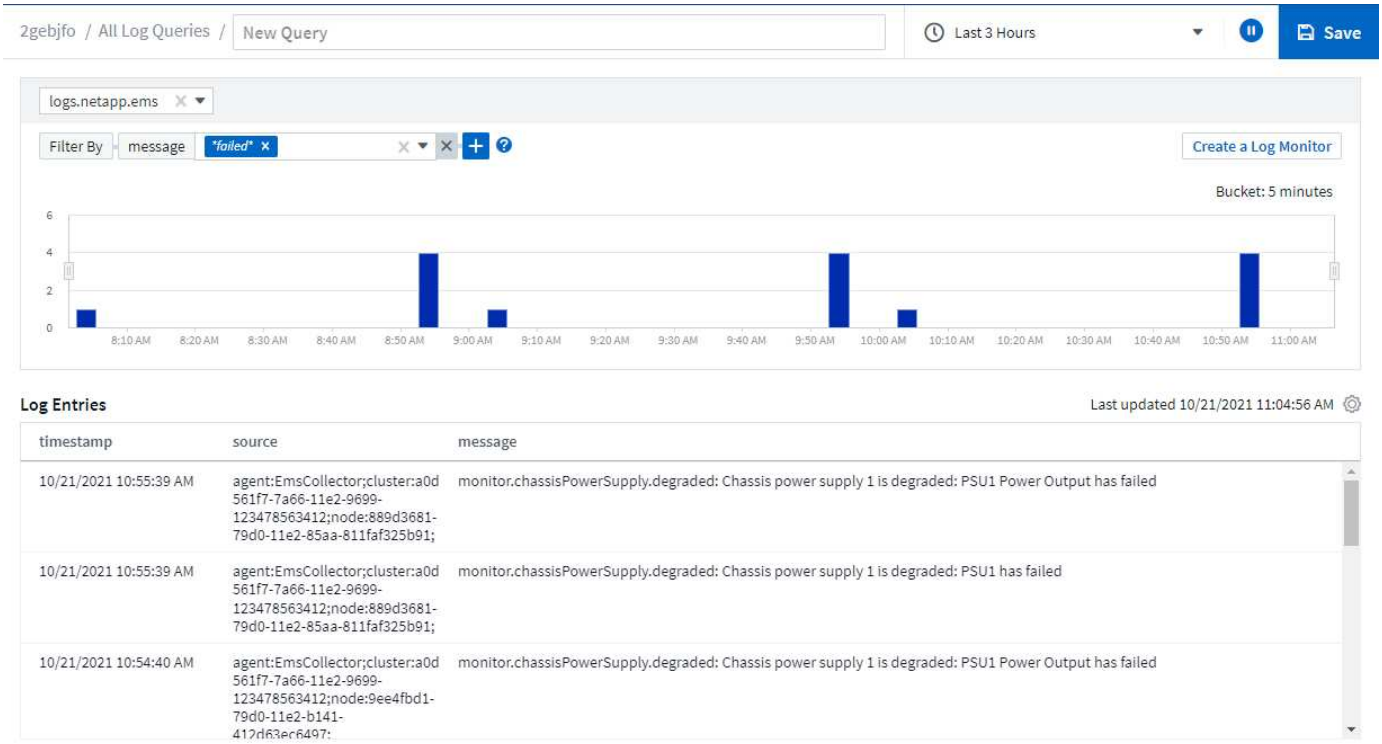


I tipi di log disponibili per le query possono variare in base all'ambiente. Nel tempo potrebbero essere aggiunti altri tipi di log.

È possibile impostare filtri per perfezionare ulteriormente i risultati della query. Ad esempio, per trovare tutti i messaggi di registro che indicano un errore, impostare un filtro per i *Messaggi* contenenti la parola "errore".

Puoi iniziare a digitare il testo desiderato nel campo filtro; Data Infrastructure Insights ti chiederà di creare una ricerca con caratteri jolly contenente la stringa mentre digiti.

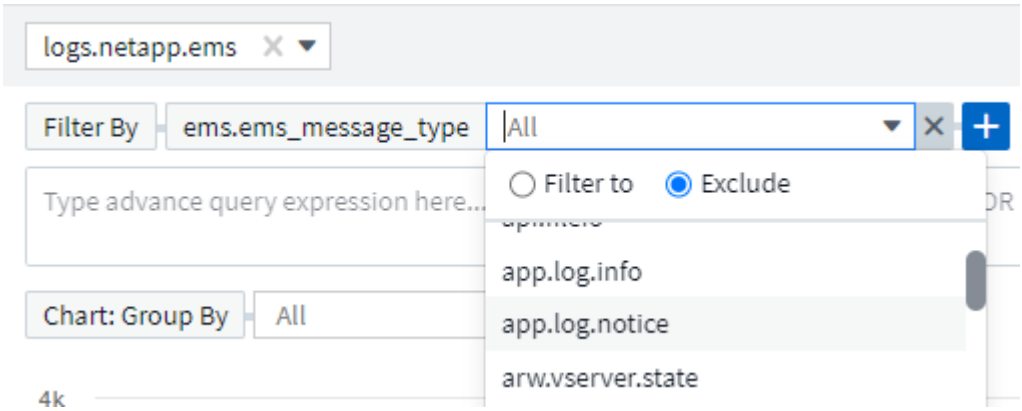
I risultati vengono visualizzati in un grafico che mostra il numero di istanze di registro in ciascun periodo di tempo mostrato. Sotto il grafico si trovano le voci di registro stesse. Il grafico e le voci si aggiornano automaticamente in base all'intervallo di tempo selezionato.



Filtraggio

Includi / Escludi

Quando si filtrano i log, è possibile scegliere di **includere** (ad esempio "Filtra per") o **escludere** le stringhe digitate. Le stringhe escluse vengono visualizzate nel filtro completato come "NOT <stringa>".



I filtri basati su caratteri jolly o espressioni (ad esempio NOT, OR, "Nessuno", ecc.) vengono visualizzati in blu scuro nel campo filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in azzurro.

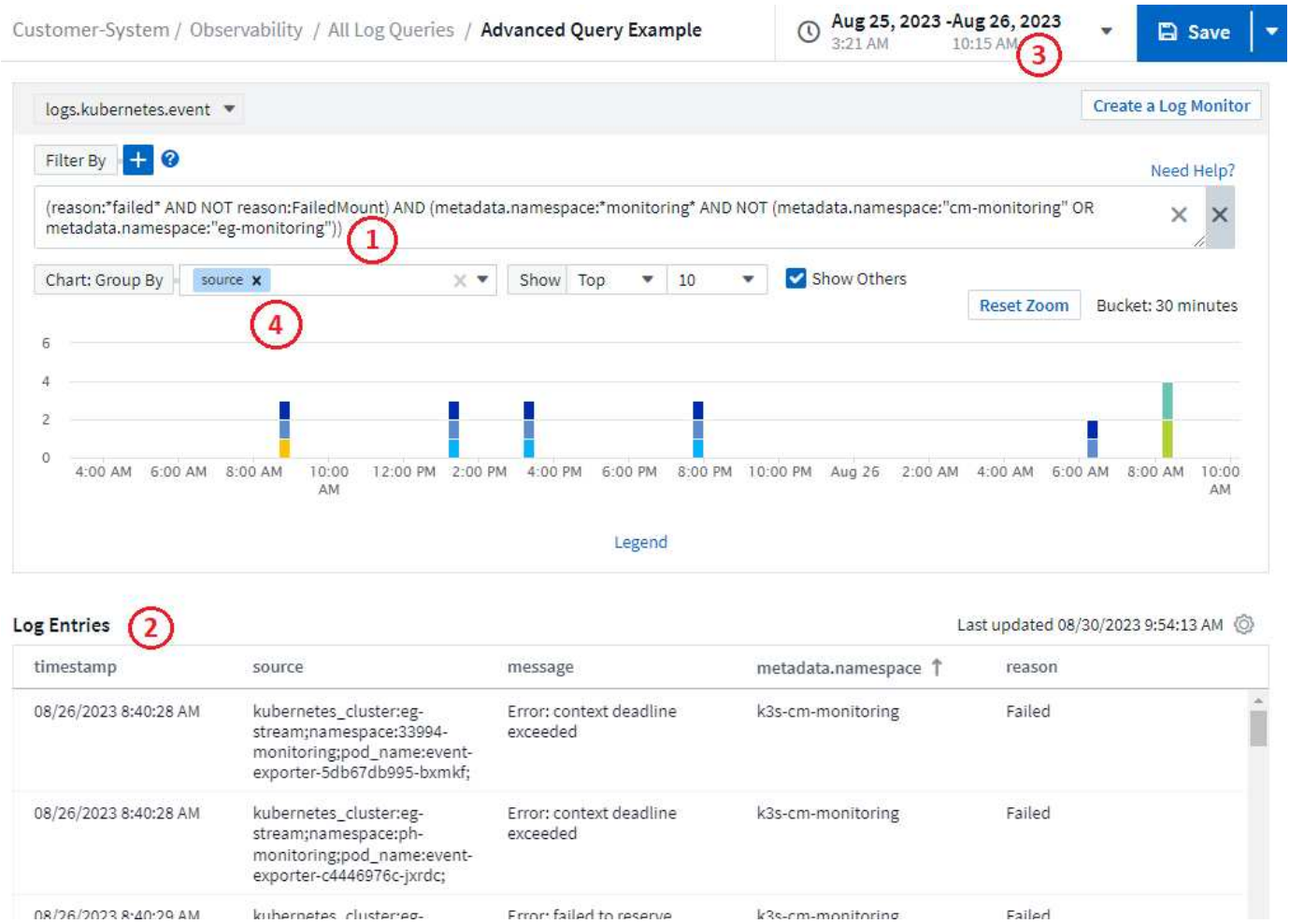
In qualsiasi momento puoi cliccare su *Crea un Log Monitor* per creare un nuovo Monitor basato sul filtro corrente.

Filtraggio avanzato

Quando si filtrano valori di testo o di elenco in query o widget della dashboard, quando si inizia a digitare viene presentata l'opzione per creare un **filtro con caratteri jolly** in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione jolly. È anche possibile creare espressioni utilizzando NOT, AND o OR, oppure selezionare l'opzione "Nessuno" per filtrare i valori nulli.

Assicurati di salvare la tua query in anticipo e spesso mentre crei il tuo filtro. Le query avanzate sono immissioni di stringhe "in formato libero" e potrebbero verificarsi errori di analisi durante la compilazione.

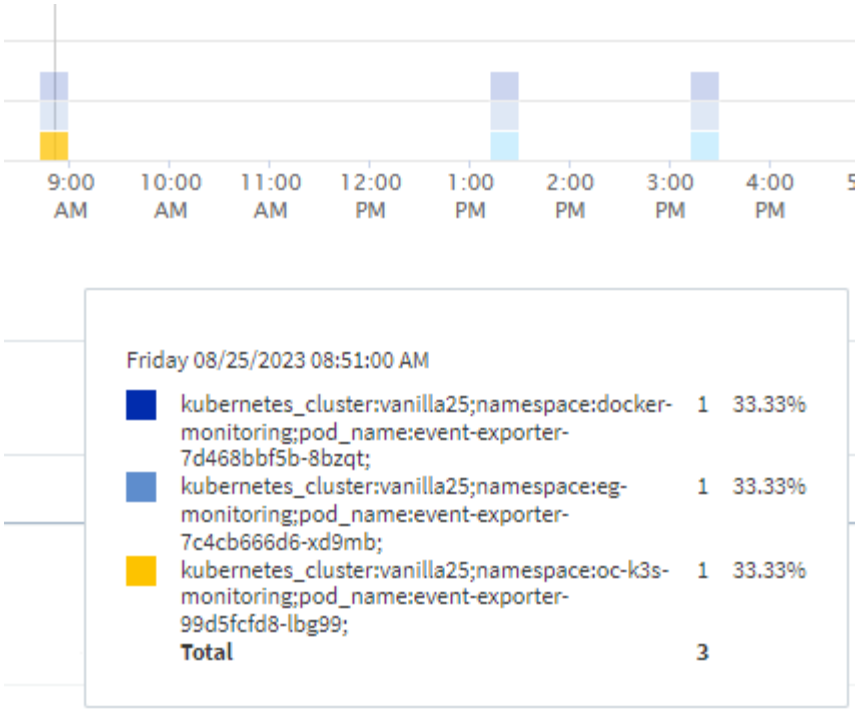
Diamo un'occhiata a questa immagine dello schermo che mostra i risultati filtrati per una query avanzata del registro *logs.kubernetes.event*. In questa pagina succedono molte cose, come spiegato sotto l'immagine:



1. Questa stringa di query avanzata filtra per quanto segue:
   - Filtra le voci di registro con un *motivo* che include la parola "failed", ma non nulla con il motivo specifico "FailedMount".
   - Includere tutte le voci che includono anche un *metadata.namespace* contenente la parola "monitoring", ma escludere gli spazi dei nomi specifici di "cm-monitoring" o "eg-monitoring".

     Si noti che nel caso sopra, poiché sia "cm-monitoring" che "eg-monitoring" contengono un trattino ("-"), le stringhe devono essere racchiuse tra virgolette doppie, altrimenti verrà visualizzato un errore di analisi. Le stringhe che non includono trattini, spazi, ecc. non devono essere racchiuse tra virgolette. In caso di dubbi, prova a mettere la stringa tra virgolette.

2. I risultati del filtro corrente, inclusi tutti i valori "Filtra per" E il filtro Query avanzata, vengono visualizzati nell'elenco dei risultati. L'elenco può essere ordinato in base a qualsiasi colonna visualizzata. Per visualizzare colonne aggiuntive, seleziona l'icona "ingranaggio".
3. Il grafico è stato ingrandito per mostrare solo i risultati del log che si sono verificati in un intervallo di tempo specifico. L'intervallo di tempo mostrato qui riflette il livello di zoom corrente. Selezionare il pulsante *Reimposta zoom* per ripristinare il livello di zoom all'intervallo di tempo corrente Data Infrastructure Insights .
4. I risultati del grafico sono stati raggruppati in base al campo *source*. Il grafico mostra i risultati in ogni colonna raggruppati per colore. Passando il mouse su una colonna del grafico verranno visualizzati alcuni dettagli sulle voci specifiche.



Filtri di affinamento

Per affinare il filtro puoi usare quanto segue:

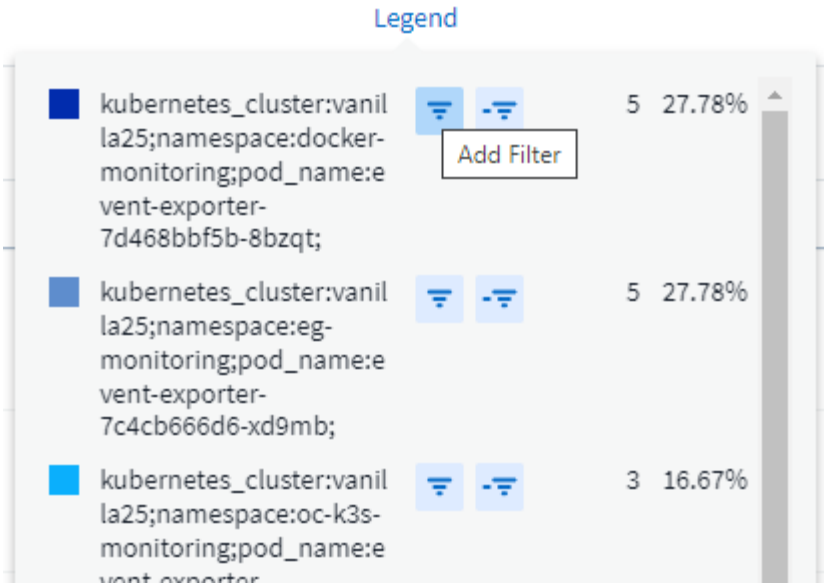
Filtro	Cosa fa
* (Asterisco)	ti permette di cercare tutto
? (punto interrogativo)	consente di cercare un numero specifico di caratteri
O	consente di specificare più entità
NON	consente di escludere il testo dai risultati della ricerca
Nessuno	cerca valori NULL in tutti i campi
Non *	cerca valori NULL nei campi *solo testo*

Se si racchiude una stringa di filtro tra virgolette doppie, Insight considera tutto ciò che si trova tra la prima e l'ultima virgoletta come una corrispondenza esatta. Tutti i caratteri speciali o gli operatori all'interno delle virgolette verranno trattati come valori letterali. Ad esempio, filtrando per "*" si otterranno risultati che sono un asterisco letterale; in questo caso l'asterisco non verrà trattato come un carattere jolly. Anche gli operatori OR e NOT verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

È possibile combinare un filtro semplice con un filtro di query avanzato; il filtro risultante è un "AND" dei due.

La legenda del grafico

Anche la *Legend* sotto il grafico riserva qualche sorpresa. Per ogni risultato (in base al filtro corrente) mostrato nella Legenda, hai la possibilità di visualizzare solo i risultati per quella riga (Aggiungi filtro) oppure di visualizzare tutti i risultati NON per quella riga (Aggiungi filtro di esclusione). Il grafico e l'elenco delle voci di registro vengono aggiornati per mostrare i risultati in base alla selezione effettuata. Per rimuovere questo filtro, aprire nuovamente la Legenda e selezionare la [X] per cancellare il filtro basato sulla Legenda.

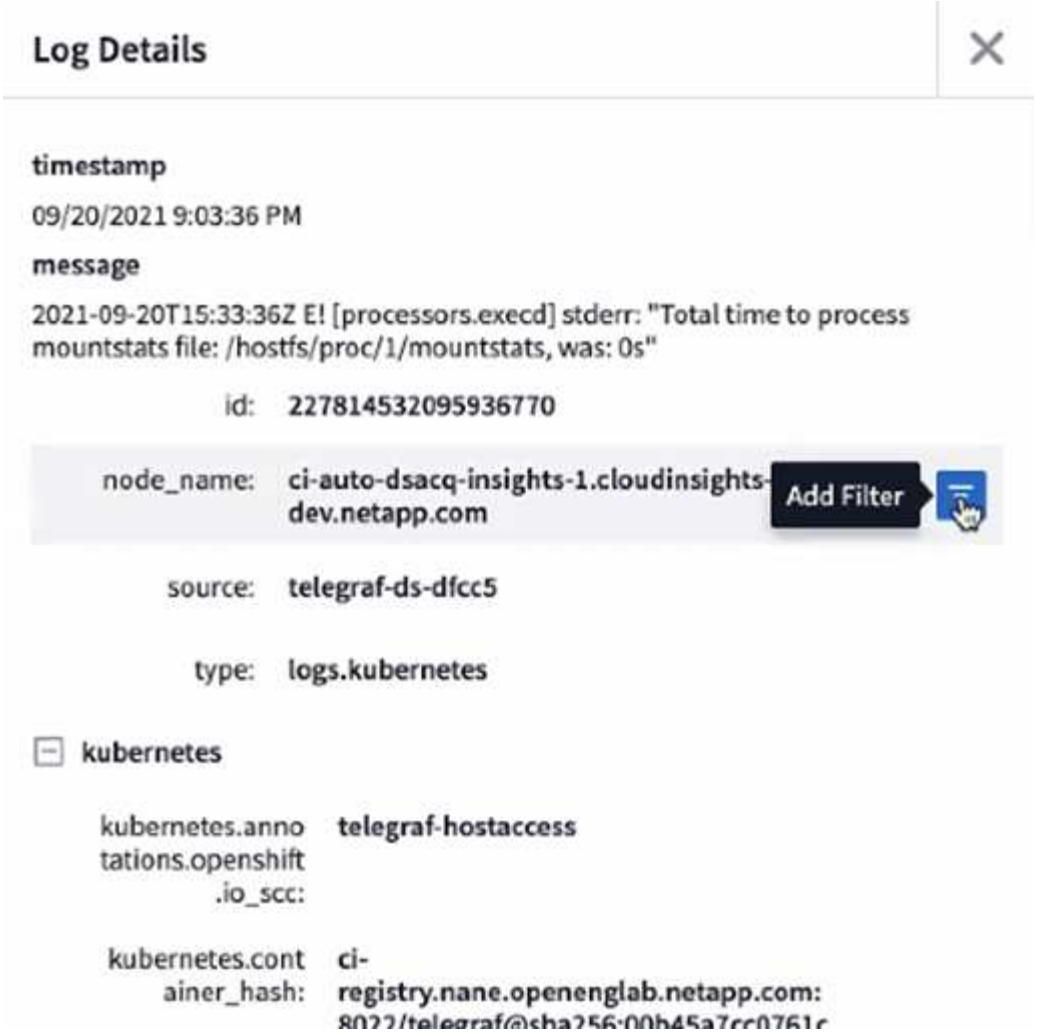


Dettagli del registro

Facendo clic in un punto qualsiasi di una voce del registro nell'elenco, si aprirà un riquadro dei dettagli per quella voce. Qui puoi trovare maggiori informazioni sull'evento.

Fare clic su "Aggiungi filtro" per aggiungere il campo selezionato al filtro corrente. L'elenco delle voci del registro verrà aggiornato in base al nuovo filtro.

Si noti che alcuni campi non possono essere aggiunti come filtri; in questi casi, l'icona *Aggiungi filtro* non è disponibile.



Risoluzione dei problemi

Qui troverete suggerimenti per la risoluzione dei problemi relativi alle query di registro.

Problema:	Prova questo:
Non vedo messaggi di "debug" nella mia query di registro	I messaggi del registro di debug non vengono raccolti. Per acquisire i messaggi desiderati, modifica la gravità del messaggio in livello *informativo, errore, avviso, emergenza* o *avviso*.

Identificazione dei dispositivi inattivi

Identificare le risorse di cui si dispone e chi le utilizza è fondamentale per "dimensionarle correttamente" e liberare infrastrutture inutilizzate. È possibile riassegnare o dismettere facilmente le risorse sottoutilizzate ed evitare acquisti non necessari.

Per identificare le risorse inattive, attenersi alla seguente procedura.

Passi

- Vai su **Osservabilità > Esplora** → **+Nuova query metrica**.
- Selezionare *Archiviazione* dal menu a discesa.

- Fare clic sull'ingranaggio e aggiungere *isActive* come colonna.

  Le righe che mostrano un segno di spunta sono attive. "X" indica i dispositivi inattivi.

Per rimuovere i dispositivi inattivi, seleziona semplicemente i dispositivi da rimuovere e nel menu a discesa **Azioni in blocco** seleziona *Elimina dispositivi inattivi*.

Approfondimenti

Approfondimenti

Gli approfondimenti consentono di analizzare aspetti quali l'utilizzo delle risorse e il modo in cui influisce su altre risorse, oppure di effettuare analisi del tempo di utilizzo completo.

Sono disponibili numerosi approfondimenti. Vai su **Dashboard > Approfondimenti** per iniziare a esplorare. Puoi visualizzare gli Approfondimenti attivi (in corso di elaborazione) nella scheda principale, oppure gli Approfondimenti inattivi nella scheda *Approfondimenti inattivi*. Gli Insight inattivi sono quelli che erano precedentemente attivi ma che non si verificano più.

Tipi di intuizione

Risorse condivise sotto stress

I carichi di lavoro ad alto impatto possono ridurre le prestazioni di altri carichi di lavoro in una risorsa condivisa. Ciò mette sotto stress la risorsa condivisa. Data Infrastructure Insights fornisce strumenti che ti aiutano a esaminare la saturazione delle risorse e l'impatto sul tuo tenant."Saperne di più"

Gli spazi dei nomi di Kubernetes stanno esaurendo lo spazio

Kubernetes Namespaces Running Out of Space Insight fornisce una panoramica dei carichi di lavoro sui namespace Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si riempia."Saperne di più"

Reclaim ONTAP Cold Storage

Reclaim ONTAP Cold Storage Insight fornisce dati sulla capacità di raffreddamento, sui potenziali risparmi in termini di costi/energia e sulle azioni consigliate per i volumi sui sistemi ONTAP ."Saperne di più"

> Questa è una funzionalità di *Anteprima* e potrebbe cambiare nel tempo man mano che vengono apportati miglioramenti. "Saperne di più" Informazioni sulle funzionalità di Data Infrastructure Insights Preview.

Approfondimenti: risorse condivise sotto stress

I carichi di lavoro ad alto impatto possono ridurre le prestazioni di altri carichi di lavoro in una risorsa condivisa. Ciò mette sotto stress la risorsa condivisa. Data Infrastructure Insights fornisce strumenti che ti aiutano a esaminare la saturazione delle risorse e l'impatto sul tuo tenant.

Terminologia

Quando si parla di carico di lavoro o di impatto sulle risorse, le seguenti definizioni sono utili.

Un **carico di lavoro impegnativo** è un carico di lavoro che attualmente è identificato come avente un impatto su altre risorse nel pool di archiviazione condiviso. Questi carichi di lavoro determinano IOPS più elevati (ad esempio), riducendo gli IOPS nei carichi di lavoro interessati. I carichi di lavoro impegnativi sono talvolta chiamati *carichi di lavoro ad alto consumo*.

Un **carico di lavoro interessato** è un carico di lavoro che è influenzato da un carico di lavoro ad alto consumo nel pool di archiviazione condiviso. Questi carichi di lavoro presentano IOPS ridotti e/o latenza più elevata, causati dai carichi di lavoro impegnativi.

Si noti che se Data Infrastructure Insights non ha rilevato il carico di lavoro di elaborazione principale, il volume o il volume interno stesso verrà riconosciuto come carico di lavoro. Ciò vale sia per i carichi di lavoro impegnativi che per quelli con impatto.

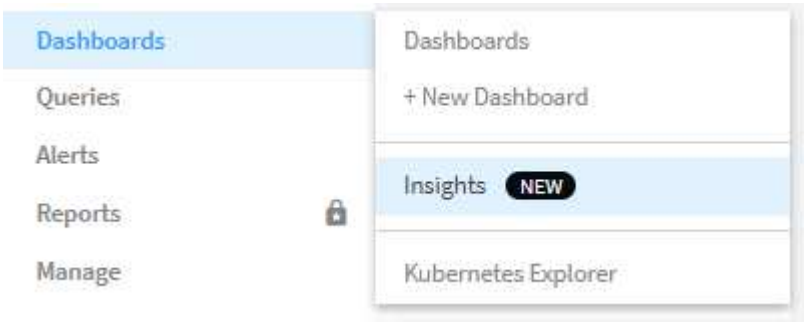
Saturazione delle risorse condivise è il rapporto tra IOPS impattanti e *baseline*.

Baseline è definito come il punto dati massimo riportato per ciascun carico di lavoro nell'ora immediatamente precedente la saturazione rilevata.

Si verifica una **contesa** o una **saturazione** quando si determina che gli IOPS stanno influenzando altre risorse o carichi di lavoro nel pool di archiviazione condiviso.

Carichi di lavoro impegnativi

Per iniziare a esaminare i carichi di lavoro impegnativi e interessati nelle risorse condivise, fare clic su **Dashboard > Approfondimenti** e selezionare l'approfondimento **Risorse condivise sotto stress**.



Data Infrastructure Insights visualizza un elenco di tutti i carichi di lavoro in cui è stata rilevata una saturazione. Si noti che Data Infrastructure Insights mostrerà i carichi di lavoro in cui è stata rilevata almeno una *risorsa impegnativa* **o** una *risorsa interessata*.

Fare clic su un carico di lavoro per visualizzarne la pagina dei dettagli. Il grafico in alto mostra l'attività sulla risorsa condivisa (ad esempio, un pool di archiviazione) su cui si verifica la contesa/saturazione.

Di seguito sono riportati due grafici che mostrano i carichi di lavoro *impegnativi* e i carichi di lavoro che sono *influenzati* da tali carichi di lavoro.

Sotto ogni tabella è presente un elenco dei carichi di lavoro e/o delle risorse che incidono o sono interessati dalla contesa. Facendo clic su una risorsa (ad esempio, una VM) si apre una pagina dei dettagli per quella risorsa. Facendo clic su un carico di lavoro si apre una pagina di query che mostra i pod coinvolti. Tieni presente che se il collegamento apre una query vuota, potrebbe essere perché il pod interessato non fa più parte della contesa attiva. È possibile modificare l'intervallo di tempo della query per visualizzare l'elenco dei pod in un intervallo di tempo più ampio o più mirato.

Cosa posso fare per risolvere il problema della saturazione?

Esistono diversi accorgimenti che puoi adottare per ridurre o eliminare il rischio di saturazione del tuo inquilino.

Per visualizzarli, espandere il link **+Mostra suggerimenti** nella pagina. Ecco alcune cose che puoi provare.

- Spostare i consumatori con IOPS elevati

  Spostare i carichi di lavoro "avidi" in pool di archiviazione meno saturi. Si consiglia di valutare il livello e la capacità di questi pool prima di spostare i carichi di lavoro, per evitare costi inutili o ulteriori conflitti.

- Implementare una politica di qualità del servizio (QoS)

  L'implementazione di una policy QoS per ogni carico di lavoro per garantire la disponibilità di risorse libere sufficienti allevierà la saturazione del pool di archiviazione. Questa è una soluzione a lungo termine.

- Aggiungi risorse aggiuntive

  Se la risorsa condivisa (ad esempio, Storage Pool) ha raggiunto il punto di saturazione IOPS, l'aggiunta di dischi più numerosi o più veloci al pool garantirà la disponibilità di risorse libere sufficienti per alleviare la saturazione.

Infine, puoi cliccare su **Copia collegamento Insight** per copiare l'URL della pagina negli appunti e condividerlo più facilmente con i colleghi.

Approfondimenti: gli spazi dei nomi di Kubernetes stanno esaurendo lo spazio

Rimanere senza spazio sul proprio inquilino non è mai una bella situazione. Data Infrastructure Insights ti aiuta a prevedere quanto tempo hai a disposizione prima che i volumi persistenti di Kubernetes si riempiano.

L'Insight *Kubernetes Namespaces Running Out of Space* fornisce una panoramica dei carichi di lavoro sui namespace Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni volume persistente si riempia.

Puoi visualizzare questa Insight andando su **Dashboard > Insight**.

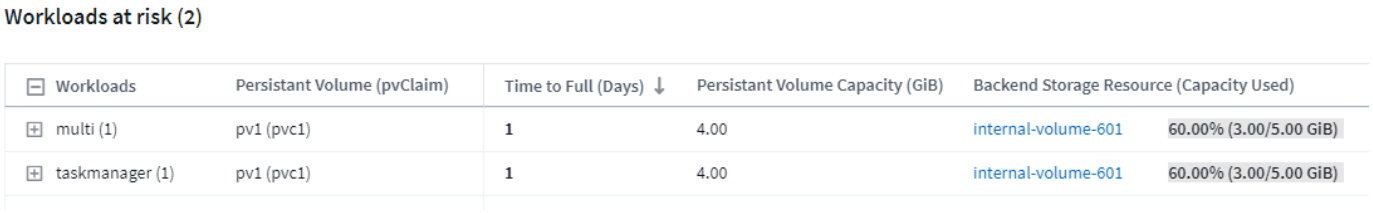
Kubernetes Namespaces Running Out of Space (3)

Description	Estimated Days to Full	Workloads at Risk	Detected ↓
1 workload at risk on es	35	1	2 days ago
1 workload at risk on manager	24	1	2 days ago
2 workloads at risk on cloudinsights	1	2	2 days ago

Fare clic su un carico di lavoro per aprire una pagina dettagliata per Insight. In questa pagina vedrai un grafico che mostra le tendenze della capacità del carico di lavoro e una tabella che mostra quanto segue:

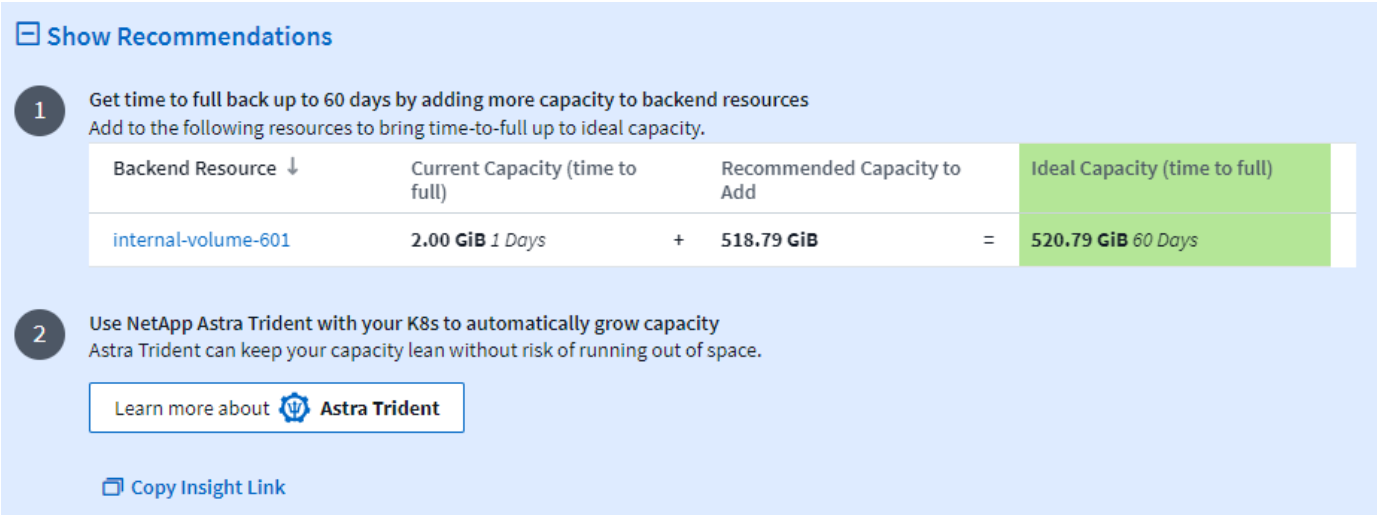
- Nome del carico di lavoro
- Volume persistente interessato
- Tempo previsto per il completamento in giorni
- Capacità di volume persistente

- Risorsa di archiviazione back-end interessata, con capacità corrente utilizzata rispetto alla capacità totale. Facendo clic su questo collegamento si aprirà la pagina di destinazione dettagliata per il volume backend.



Cosa posso fare se sto esaurendo lo spazio?

Nella pagina Insight, fare clic su **+Mostra suggerimenti** per visualizzare le possibili soluzioni. L'opzione più semplice quando lo spazio si esaurisce è sempre quella di aggiungere più capacità. Data Infrastructure Insights mostra la capacità ottimale da aggiungere per aumentare il tempo di riempimento fino a una previsione target di 60 giorni. Vengono mostrate anche altre raccomandazioni.



Qui puoi anche copiare un comodo collegamento a questa Insight, per aggiungere la pagina ai preferiti o per condividerla facilmente con il tuo team.

Approfondimenti: Reclaim ONTAP Cold Storage

Reclaim ONTAP Cold Storage Insight fornisce dati sulla capacità di raffreddamento, sui potenziali risparmi in termini di costi/energia e sulle azioni consigliate per i volumi sui sistemi ONTAP .

Per visualizzare queste informazioni, vai su **Dashboard > Informazioni** e dai un'occhiata all'Insight *Reclaim ONTAP Cold Storage*. Tieni presente che questa Insight elencherà gli archivi interessati solo se Data Infrastructure Insights ha rilevato un archivio cold, altrimenti verrà visualizzato un messaggio di "tutto a posto".

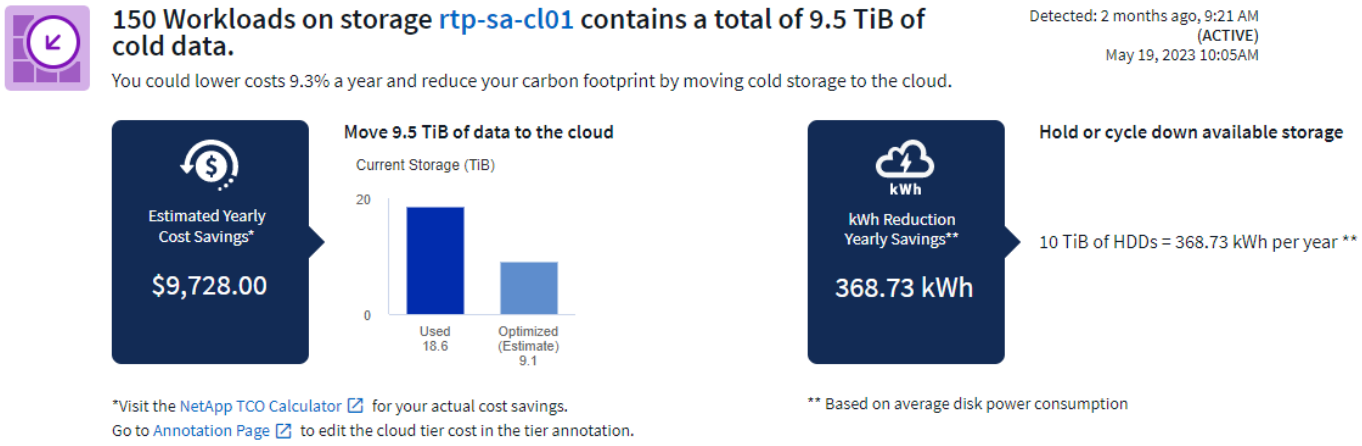
Tieni presente che i dati inattivi risalenti a meno di 30 giorni fa non vengono visualizzati.

Reclaim ONTAP Cold Storage (3)

Description	Cold data storage(TiB)	Workloads with cold data	Detected ↓
0.30 TiB of cold data on storage rtp-sa-cl04	0.30	45	an hour ago
1.22 TiB of cold data on storage umeng-aff300-01-02	1.22	84	16 days ago
11.62 TiB of cold data on storage rtp-sa-cl01	11.62	171	16 days ago

La descrizione di Insight fornisce una rapida indicazione della quantità di dati rilevati come "freddi" e su quale storage risiedono tali dati. La tabella fornisce anche un conteggio dei carichi di lavoro con dati inattivi.

Selezionando un'Insight dall'elenco si apre una pagina che mostra maggiori dettagli, tra cui consigli per spostare i dati sul cloud o disattivare i dischi unificati, nonché una stima dei costi e dei risparmi energetici che potresti potenzialmente ottenere implementando tali consigli. La pagina fornisce anche un comodo collegamento a"Calcolatore TCO di NetApp" così puoi sperimentare con i numeri.



Raccomandazioni

Nella pagina Insight, espandi **Raccomandazioni** per esplorare le seguenti opzioni:

- Spostare i carichi di lavoro inutilizzati (zombie) su un livello di archiviazione (HDD) a costo inferiore

  Utilizzando il flag zombie, l'archiviazione a freddo e il numero di giorni, trova la quantità di dati più grande e più fredda e sposta il carico di lavoro su un livello di archiviazione a costo inferiore (ad esempio un pool di archiviazione che utilizza l'archiviazione su disco rigido). Un carico di lavoro è considerato "zombie" quando non riceve richieste di I/O significative per 30 giorni o più.

- Elimina i carichi di lavoro non utilizzati

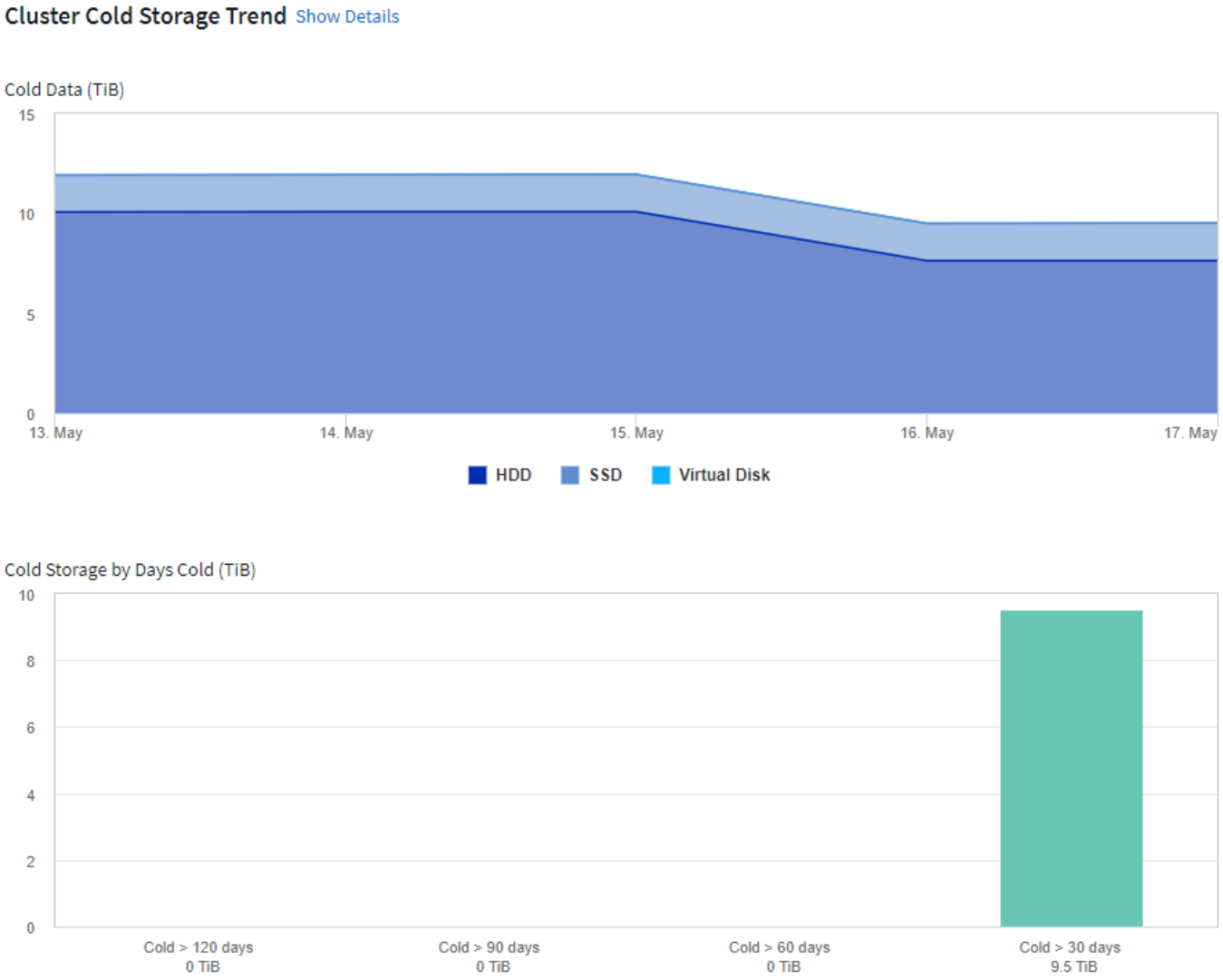
  Verificare quali carichi di lavoro non sono in uso e valutare la possibilità di archiviarli o rimuoverli dal sistema di archiviazione.

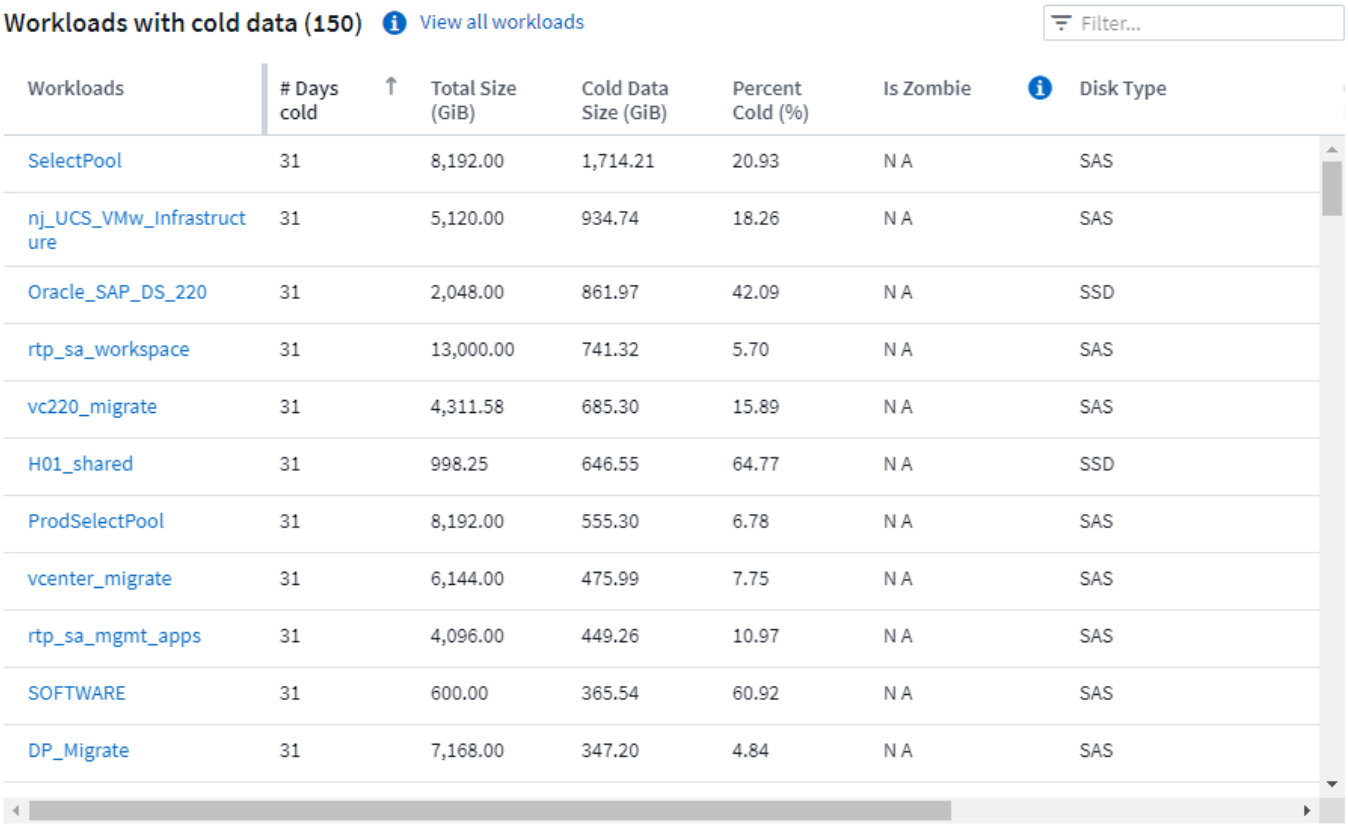
- Prendi in considerazione la soluzione Fabric Pool di NetApp

  NetApp"Soluzione per piscina in tessuto" suddivide automaticamente i dati inutilizzati in un archivio cloud a basso costo, aumentando così l'efficienza del livello di prestazioni e garantendo la protezione dei dati in remoto.

Visualizza ed esplora

I grafici e la tabella forniscono ulteriori informazioni sulle tendenze e consentono di analizzare nel dettaglio i singoli carichi di lavoro.





Monitor e avvisi

Avvisi con monitor

Configura i monitor per monitorare le soglie di prestazione, registrare eventi e anomalie nelle risorse della tua infrastruttura. Crea avvisi personalizzati per parametri quali latenza di scrittura del nodo, capacità di archiviazione o prestazioni dell'applicazione e ricevi notifiche quando queste condizioni vengono soddisfatte.

I monitor consentono di impostare soglie sulle metriche generate da oggetti "infrastrutturali" quali storage, VM, EC2 e porte, nonché per dati di "integrazione" come quelli raccolti per Kubernetes, metriche avanzate ONTAP e plugin Telegraf. Questi monitor *metrici* ti avvisano quando vengono superate le soglie di livello di attenzione o di livello critico.

È anche possibile creare monitor per attivare avvisi di livello di avvertenza, critici o informativi quando vengono rilevati specifici *eventi di registro*.

Data Infrastructure Insights fornisce una serie di"Monitor definiti dal sistema" anche in base all'ambiente.

Migliori pratiche di sicurezza

Gli avvisi di Data Infrastructure Insights sono progettati per evidenziare punti dati e tendenze sul tenant e Data Infrastructure Insights consente di immettere qualsiasi indirizzo e-mail valido come destinatario dell'avviso. Se lavori in un ambiente sicuro, fai particolare attenzione a chi riceve la notifica o ha accesso all'avviso.

Monitoraggio metrico o log?

1. Dal menu Data Infrastructure Insights , fare clic su **Avvisi > Gestisci monitoraggi**

   Viene visualizzata la pagina Elenco monitor, che mostra i monitor attualmente configurati.

2. Per modificare un monitor esistente, fare clic sul nome del monitor nell'elenco.
3. Per aggiungere un monitor, fare clic su **+ Monitor**.

   Quando si aggiunge un nuovo monitor, viene richiesto di creare un monitor delle metriche o un monitor dei registri.

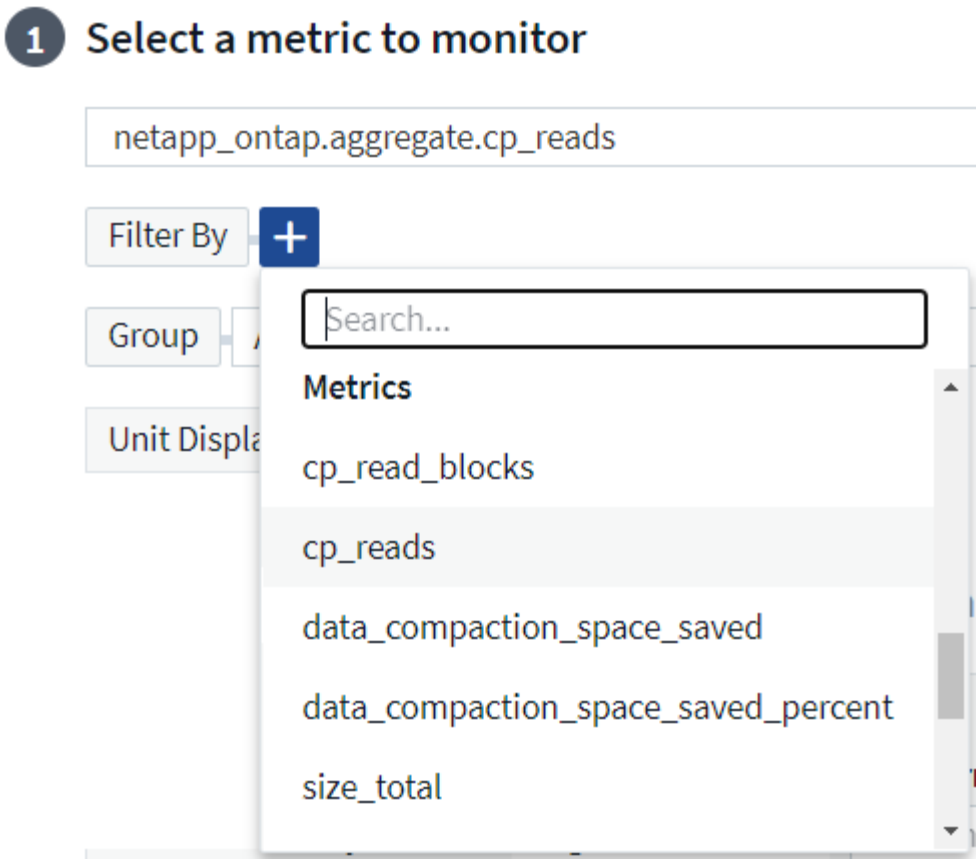
   - *Metric* monitora gli avvisi sui trigger correlati all'infrastruttura o alle prestazioni
   - *Log* monitora gli avvisi sulle attività correlate al registro

   Dopo aver scelto il tipo di monitor, viene visualizzata la finestra di dialogo Configurazione monitor. La configurazione varia a seconda del tipo di monitor che si desidera creare.

Monitor metrico

1. Nel menu a discesa, cerca e scegli un tipo di oggetto e una metrica da monitorare.

È possibile impostare filtri per restringere il campo degli attributi o delle metriche degli oggetti da monitorare.

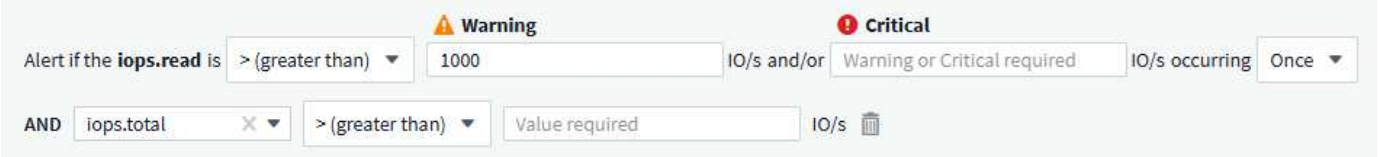


Quando si lavora con dati di integrazione (Kubernetes, ONTAP Advanced Data, ecc.), il filtraggio delle metriche rimuove i punti dati individuali/non corrispondenti dalla serie di dati tracciati, a differenza dei dati dell'infrastruttura (archiviazione, VM, porte, ecc.) in cui i filtri agiscono sul valore aggregato della serie di dati e potenzialmente rimuovono l'intero oggetto dal grafico.

I monitor delle metriche si applicano agli oggetti di inventario quali storage, switch, host, VM, ecc., nonché alle metriche di integrazione quali dati ONTAP Advanced o Kubernetes. Quando si monitorano gli oggetti dell'inventario, tenere presente che non è possibile selezionare il metodo "Raggruppa per". Tuttavia, il raggruppamento è consentito durante il monitoraggio dei dati di integrazione.

Monitor multi-condizione

Puoi scegliere di perfezionare ulteriormente il monitoraggio delle metriche aggiungendo una seconda condizione. Basta espandere il prompt "+Aggiungi condizione metrica secondaria" e configurare la condizione aggiuntiva.



Il monitor emetterà un avviso se entrambe le condizioni sono soddisfatte.

Tieni presente che puoi usare solo l'opzione "AND" per una seconda condizione; non puoi scegliere di ricevere un avviso per una condizione OPPURE per l'altra.

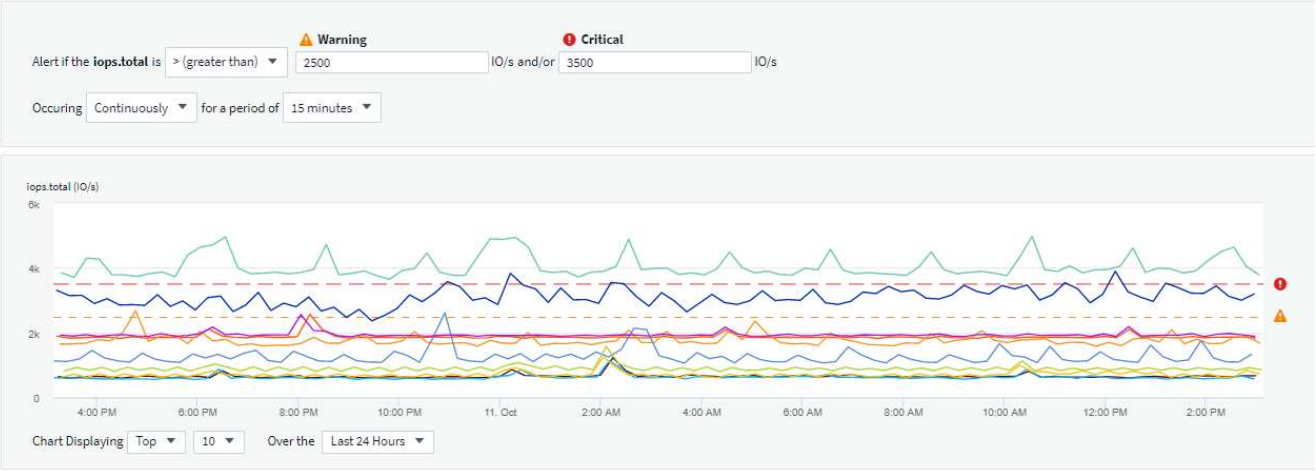
Definire le condizioni del monitor.

1. Dopo aver scelto l'oggetto e la metrica da monitorare, impostare le soglie di livello di avviso e/o di livello critico.
2. Per il livello *Avviso*, immettere 200 per il nostro esempio. La linea tratteggiata che indica questo livello di avviso viene visualizzata nel grafico di esempio.
3. Per il livello *Critico*, immettere 400. La linea tratteggiata che indica questo livello critico viene visualizzata nel grafico di esempio.

   Il grafico mostra i dati storici. Le linee di livello di avviso e critico sul grafico sono una rappresentazione visiva del Monitor, in modo da poter vedere facilmente quando il Monitor potrebbe attivare un avviso in ciascun caso.

4. Per l'intervallo di occorrenza, selezionare *Continuamente* per un periodo di *15 minuti*.

   È possibile scegliere di attivare un avviso nel momento in cui viene superata una soglia oppure attendere che la soglia venga superata in modo continuativo per un determinato periodo di tempo. Nel nostro esempio, non vogliamo essere avvisati ogni volta che il valore IOPS totale supera il livello di avviso o critico, ma solo quando un oggetto monitorato supera continuamente uno di questi livelli per almeno 15 minuti.



Definire il comportamento di risoluzione degli avvisi

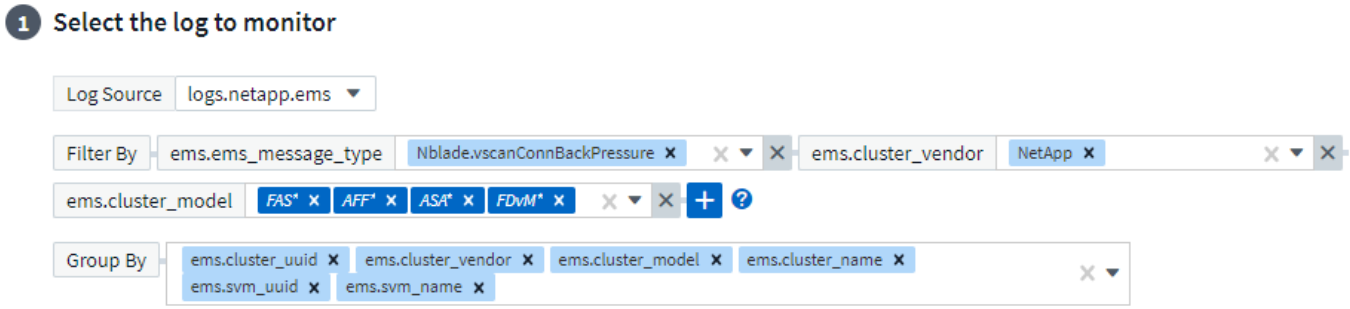
È possibile scegliere come risolvere un avviso di monitoraggio delle metriche. Ti vengono presentate due scelte:

- Risolvere quando la metrica torna nell'intervallo accettabile.
- Risolve quando la metrica rientra nell'intervallo accettabile per un periodo di tempo specificato, da 1 minuto a 7 giorni.

Monitoraggio dei registri

Quando si crea un **monitor dei log**, scegliere innanzitutto quale log monitorare dall'elenco dei log disponibili. È quindi possibile filtrare in base agli attributi disponibili come sopra. È anche possibile scegliere uno o più attributi "Raggruppa per".

Il filtro Log Monitor non può essere vuoto.



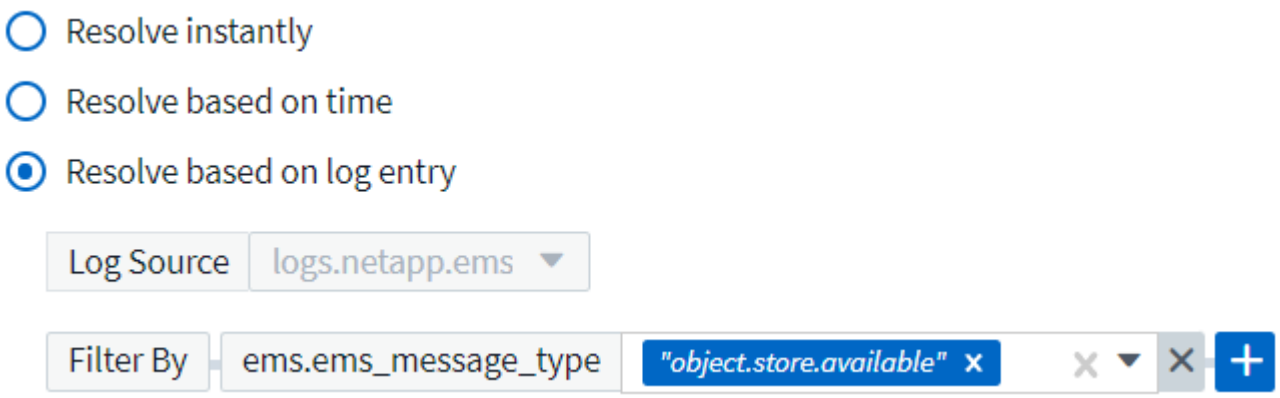
Definisci il comportamento dell'avviso

È possibile creare il monitor in modo che emetta un avviso con un livello di gravità *Critico*, *Avviso* o *Informativo* quando le condizioni definite sopra si verificano una volta (ovvero immediatamente) oppure attendere che l'avviso venga emesso finché le condizioni non si verificano 2 o più volte.

Definire il comportamento di risoluzione degli avvisi

È possibile scegliere come risolvere un avviso del monitoraggio dei log. Ti vengono presentate tre scelte:

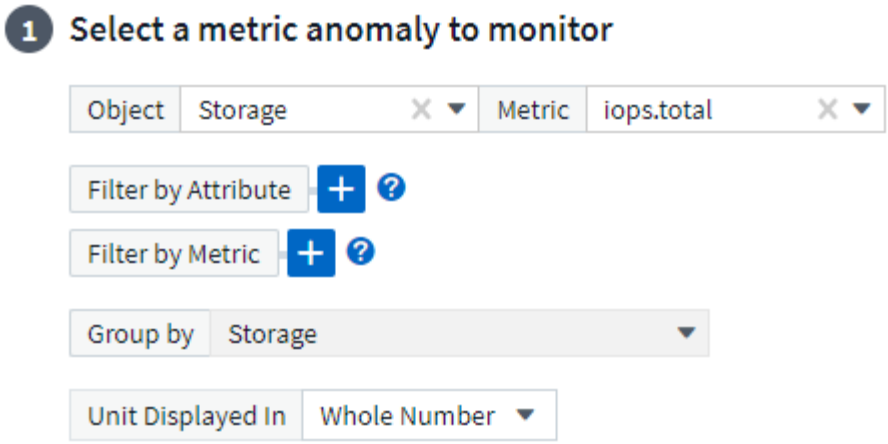
- **Risolvi istantaneamente**: l'avviso viene risolto immediatamente senza bisogno di ulteriori azioni
- **Risolvi in base al tempo**: l'avviso viene risolto dopo che è trascorso il tempo specificato
- **Risolvi in base alla voce di registro**: l'avviso viene risolto quando si verifica un'attività di registro successiva. Ad esempio, quando un oggetto viene registrato come "disponibile".



Monitoraggio del rilevamento delle anomalie

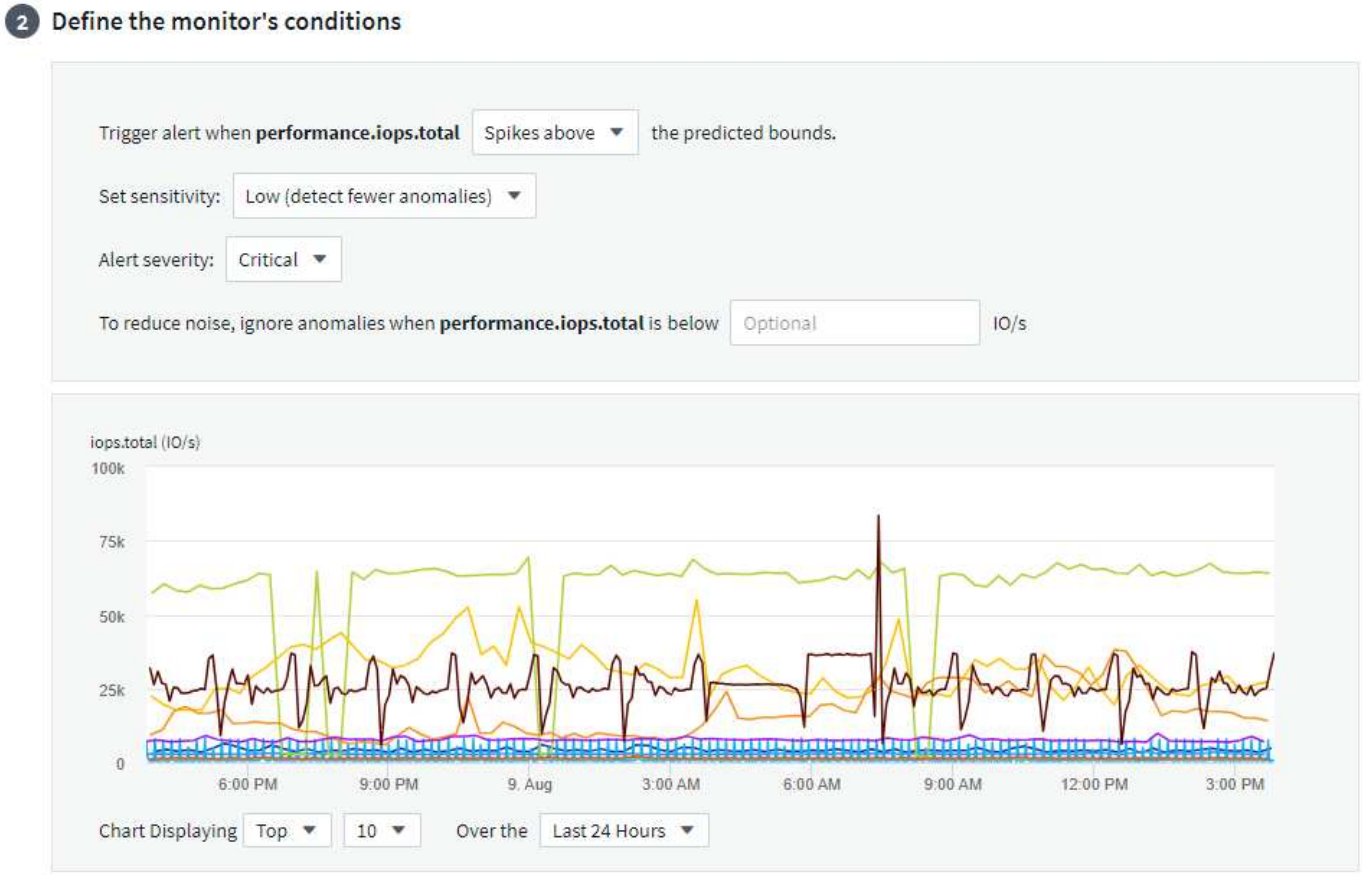
1. Nel menu a discesa, cerca e scegli un tipo di oggetto e una metrica da monitorare.

È possibile impostare filtri per restringere il campo degli attributi o delle metriche degli oggetti da monitorare.



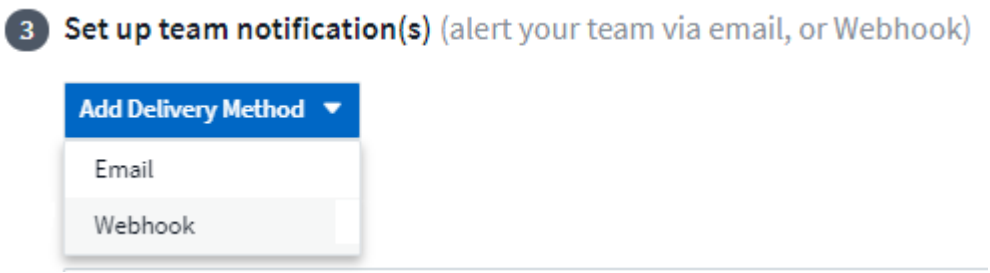
Definire le condizioni del monitor.

1. Dopo aver scelto l'oggetto e la metrica da monitorare, è necessario impostare le condizioni in cui viene rilevata un'anomalia.
   - Scegli se rilevare un'anomalia quando la metrica scelta **supera di un picco** i limiti previsti, **scende di un picco** rispetto a tali limiti oppure **supera di un picco o scende di un picco** rispetto ai limiti.
   - Imposta la **sensibilità** del rilevamento. **Basso** (vengono rilevate meno anomalie), **Medio** o **Alto** (vengono rilevate più anomalie).
   - Imposta gli avvisi come **Avviso** o **Critico**.
   - Se lo si desidera, è possibile scegliere di ridurre il rumore, ignorando le anomalie quando la metrica scelta è al di sotto di una soglia impostata.



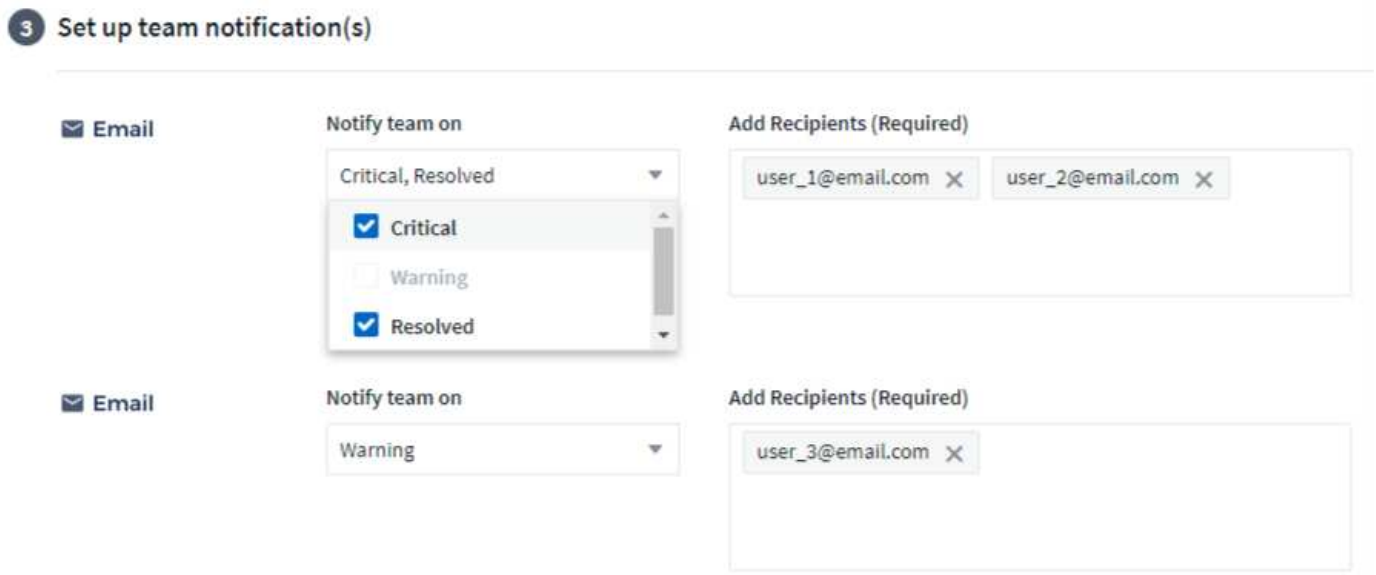
Seleziona il tipo di notifica e i destinatari

Nella sezione *Imposta notifiche al team* puoi scegliere se avvisare il tuo team tramite e-mail o Webhook.



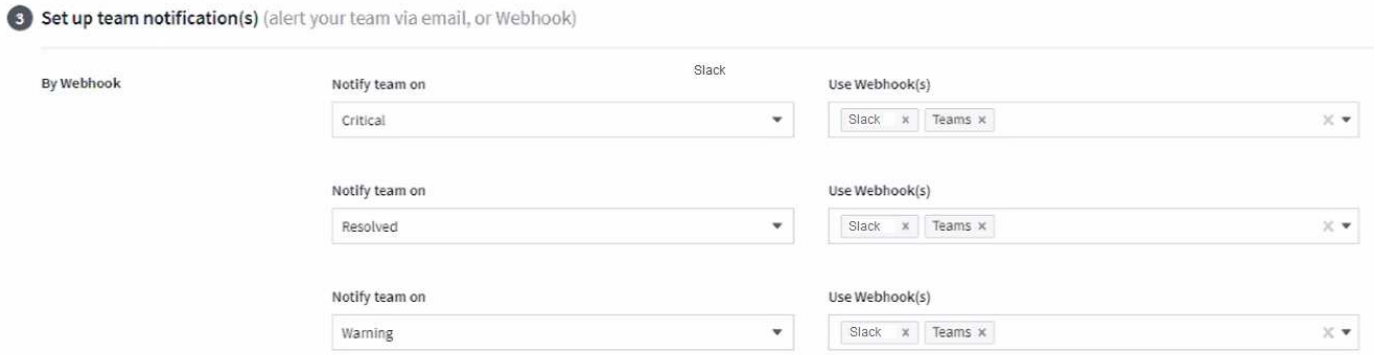
Avviso via e-mail:

Specificare i destinatari e-mail per le notifiche di avviso. Se lo desideri, puoi scegliere destinatari diversi per gli avvisi di avviso o gli avvisi critici.



Avviso tramite Webhook:

Specificare i webhook per le notifiche di avviso. Se lo desideri, puoi scegliere webhook diversi per avvisi di avviso o critici.



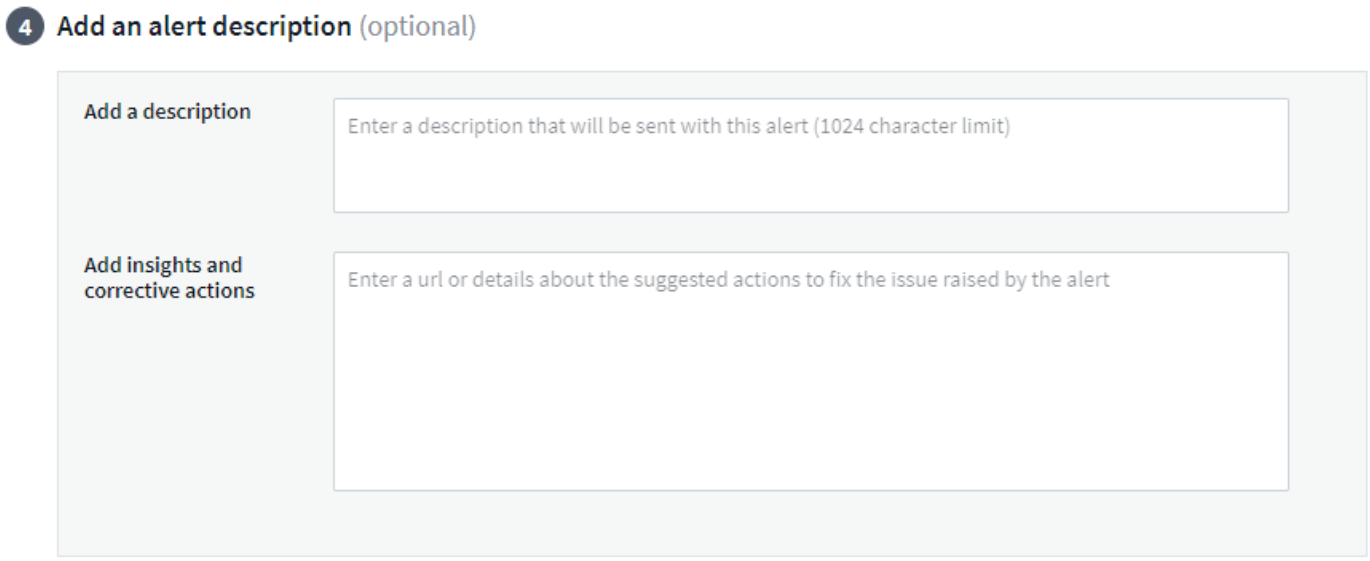
Le notifiche di ONTAP Data Collector hanno la precedenza su qualsiasi notifica specifica di Monitor pertinente al cluster/data collector. L'elenco dei destinatari impostato per il Data Collector riceverà gli avvisi del Data Collector. Se non sono presenti avvisi attivi del raccoglitore dati, gli avvisi generati dal monitor verranno inviati a destinatari specifici del monitor.

Impostazione di azioni correttive o informazioni aggiuntive

È possibile aggiungere una descrizione facoltativa, nonché ulteriori approfondimenti e/o azioni correttive compilando la sezione **Aggiungi una descrizione dell'avviso**. La descrizione può contenere fino a 1024 caratteri e verrà inviata insieme all'avviso. Il campo approfondimenti/azioni correttive può contenere fino a 67.000 caratteri e verrà visualizzato nella sezione di riepilogo della landing page dell'avviso.

In questi campi è possibile fornire note, link o passaggi da seguire per correggere o altrimenti gestire l'avviso.

È possibile aggiungere qualsiasi attributo dell'oggetto (ad esempio, il nome dell'archivio) come parametro alla descrizione di un avviso. Ad esempio, è possibile impostare i parametri per il nome del volume e il nome dell'archiviazione in una descrizione come: "Latenza elevata per volume: *%%relatedObject.volume.name%%*, Archiviazione: *%%relatedObject.storage.name%%*".



Salva il tuo monitor

1. Se lo si desidera, è possibile aggiungere una descrizione del monitor.
2. Assegna al monitor un nome significativo e fai clic su **Salva**.

   Il nuovo monitor viene aggiunto all'elenco dei monitor attivi.

Elenco monitor

La pagina Monitor elenca i monitor attualmente configurati, mostrando quanto segue:

- Nome del monitor
- Stato
- Oggetto/metrica monitorata
- Condizioni del monitor

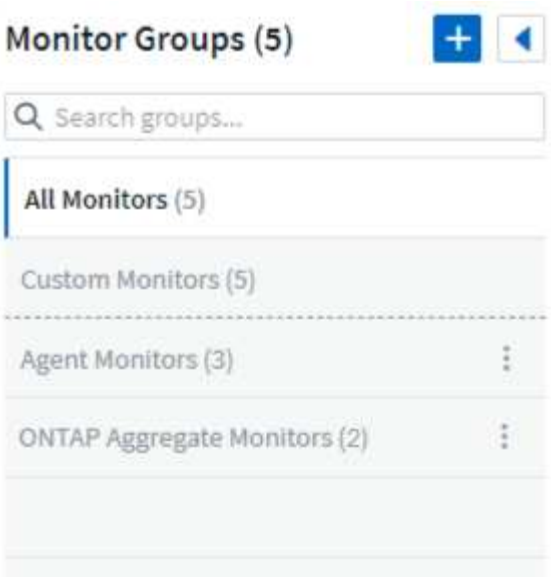
È possibile scegliere di sospendere temporaneamente il monitoraggio di un tipo di oggetto facendo clic sul menu a destra del monitor e selezionando **Pausa**. Quando sei pronto a riprendere il monitoraggio, fai clic su **Riprendi**.

È possibile copiare un monitor selezionando **Duplica** dal menu. È quindi possibile modificare il nuovo monitor e cambiare l'oggetto/la metrica, il filtro, le condizioni, i destinatari delle e-mail, ecc.

Se un monitor non è più necessario, è possibile eliminarlo selezionando **Elimina** dal menu.

Gruppi di monitoraggio

Il raggruppamento consente di visualizzare e gestire i monitor correlati. Ad esempio, è possibile avere un gruppo di monitoraggio dedicato all'archiviazione sul tenant oppure monitor rilevanti per un determinato elenco di destinatari.



Vengono mostrati i seguenti gruppi di monitor. Il numero di monitor contenuti in un gruppo è visualizzato accanto al nome del gruppo.

- **Tutti i monitor** elenca tutti i monitor.
- **Monitor personalizzati** elenca tutti i monitor creati dall'utente.
- **Monitor sospesi** elencherà tutti i monitor di sistema sospesi da Data Infrastructure Insights.
- Data Infrastructure Insights mostrerà anche un numero di **Gruppi di monitoraggio del sistema**, che elencheranno uno o più gruppi di"monitor definiti dal sistema" , inclusi i monitor di infrastruttura e carico di lavoro ONTAP .

I monitor personalizzati possono essere messi in pausa, ripresi, eliminati o spostati in un altro gruppo. I monitor definiti dal sistema possono essere messi in pausa e ripresi, ma non possono essere eliminati o spostati.

Monitor sospesi

Questo gruppo verrà visualizzato solo se Data Infrastructure Insights ha sospeso uno o più monitor. Un monitor può essere sospeso se genera avvisi eccessivi o continui. Se il monitor è personalizzato, modificare le condizioni per impedire l'avviso continuo, quindi riprendere il monitor. Il monitor verrà rimosso dal gruppo Monitor sospesi quando il problema che causa la sospensione sarà risolto.

Monitor definiti dal sistema

Questi gruppi mostreranno i monitor forniti da Data Infrastructure Insights, a condizione che l'ambiente contenga i dispositivi e/o la disponibilità dei registri richiesti dai monitor.

I monitor definiti dal sistema non possono essere modificati, spostati in un altro gruppo o eliminati. Tuttavia, è possibile duplicare un monitor di sistema e modificare o spostare il duplicato.

I monitor di sistema possono includere monitor per l'infrastruttura ONTAP (archiviazione, volume, ecc.) o carichi di lavoro (ad esempio monitor di log) o altri gruppi. NetApp valuta costantemente le esigenze dei clienti e le funzionalità dei prodotti e, se necessario, aggiorna o aggiunge funzionalità ai monitor e ai gruppi di sistema.

Gruppi di monitor personalizzati

È possibile creare gruppi personalizzati in cui inserire i monitor in base alle proprie esigenze. Ad esempio, potresti voler creare un gruppo per tutti i monitor correlati all'archiviazione.

Per creare un nuovo gruppo di monitor personalizzato, fare clic sul pulsante **"+" Crea nuovo gruppo di monitor**. Inserisci un nome per il gruppo e clicca su **Crea gruppo**. Viene creato un gruppo vuoto con quel nome.

Per aggiungere monitor al gruppo, vai al gruppo *Tutti i monitor* (consigliato) ed esegui una delle seguenti operazioni:

- Per aggiungere un singolo monitor, fare clic sul menu a destra del monitor e selezionare *Aggiungi al gruppo*. Selezionare il gruppo a cui aggiungere il monitor.
- Fare clic sul nome del monitor per aprire la vista di modifica del monitor e selezionare un gruppo nella sezione *Associa a un gruppo di monitor*.

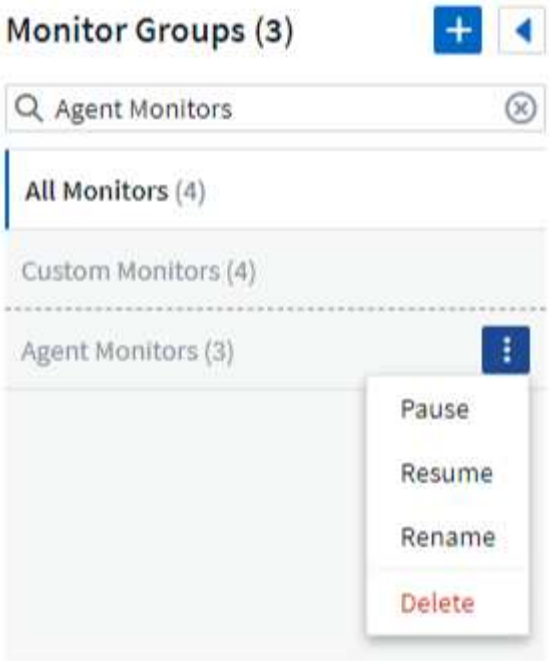
Per rimuovere i monitor, fare clic su un gruppo e selezionare *Rimuovi dal gruppo* dal menu. Non è possibile rimuovere i monitor dal gruppo *Tutti i monitor* o *Monitor personalizzati*. Per eliminare un monitor da questi gruppi, è necessario eliminare il monitor stesso.

> La rimozione di un monitor da un gruppo non elimina il monitor da Data Infrastructure Insights. Per rimuovere completamente un monitor, selezionarlo e fare clic su *Elimina*. In questo modo l'utente verrà rimosso anche dal gruppo a cui apparteneva e non sarà più disponibile per nessun altro utente.

È anche possibile spostare un monitor in un gruppo diverso nello stesso modo, selezionando *Sposta nel gruppo*.

Per mettere in pausa o riprendere contemporaneamente tutti i monitor di un gruppo, selezionare il menu del gruppo e fare clic su *Pausa* o *Riprendi*.

Utilizzare lo stesso menu per rinominare o eliminare un gruppo. L'eliminazione di un gruppo non elimina i monitor da Data Infrastructure Insights; sono comunque disponibili in *Tutti i monitor*.



Monitor definiti dal sistema

Data Infrastructure Insights include una serie di monitor definiti dal sistema sia per le metriche che per i log. I monitor di sistema disponibili dipendono dai collettori di dati presenti sul tenant. Per questo motivo, i monitor disponibili in Data Infrastructure Insights potrebbero cambiare man mano che vengono aggiunti raccoglitori di dati o ne vengono modificate le configurazioni.

Visualizza il"Monitor definiti dal sistema" pagina per le descrizioni dei monitor inclusi in Data Infrastructure Insights.

Ulteriori informazioni

- "Visualizzazione e chiusura degli avvisi"

Visualizzazione e gestione degli avvisi dai monitor

Data Infrastructure Insights visualizza avvisi quando"soglie monitorate" vengono superati.

Monitor e avvisi sono disponibili in Data Infrastructure Insights Standard Edition e versioni successive.

Visualizzazione e gestione degli avvisi

Per visualizzare e gestire gli avvisi, procedere come segue.

1. Vai alla pagina **Avvisi > Tutti gli avvisi**.
2. Viene visualizzato un elenco contenente fino ai 1.000 avvisi più recenti. È possibile ordinare questo elenco in base a qualsiasi campo facendo clic sull'intestazione della colonna corrispondente. L'elenco visualizza le seguenti informazioni. Si noti che non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare cliccando sull'icona "ingranaggio":
   - **ID avviso**: ID avviso univoco generato dal sistema

- **Ora di attivazione**: l'ora in cui il monitor pertinente ha attivato l'avviso
- **Gravità attuale** (scheda Avvisi attivi): la gravità attuale dell'avviso attivo
- **Gravità massima** (scheda Avvisi risolti); la gravità massima dell'avviso prima che venisse risolto
- **Monitor**: Il monitor configurato per attivare l'avviso
- **Attivato su**: l'oggetto su cui è stata superata la soglia monitorata
- **Stato**: Stato attuale dell'avviso, *Nuovo* o *In elaborazione*
- **Stato attivo**: *Attivo* o *Risolto*
- **Condizione**: la condizione di soglia che ha attivato l'avviso
- **Metrica**: la metrica dell'oggetto su cui è stata superata la soglia monitorata
- **Stato del monitor**: Stato attuale del monitor che ha attivato l'avviso
- **Ha un'azione correttiva**: l'avviso ha suggerito azioni correttive. Per visualizzarli, apri la pagina degli avvisi.

È possibile gestire un avviso cliccando sul menu a destra dell'avviso e scegliendo una delle seguenti opzioni:

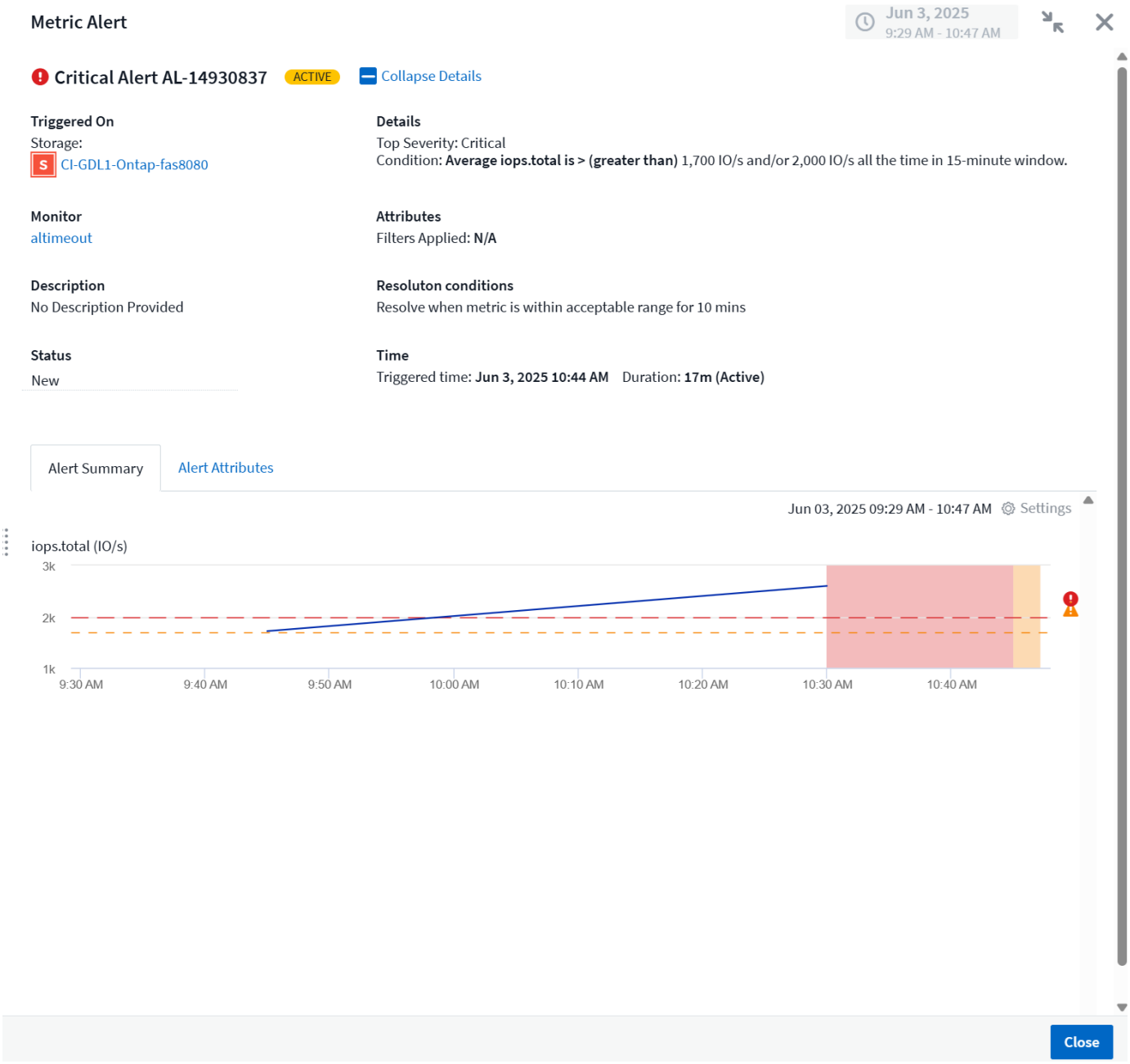
- **In corso** per indicare che l'avviso è sotto inchiesta o che deve comunque essere mantenuto aperto
- **Ignora** per rimuovere l'avviso dall'elenco degli avvisi attivi.

È possibile gestire più avvisi selezionando la casella di controllo a sinistra di ciascun avviso e facendo clic su *Modifica stato avvisi selezionati*.

Facendo clic su un ID avviso si apre la pagina dei dettagli dell'avviso.

Pannello dettagli avviso

Selezionare una riga di avviso per aprire il pannello dei dettagli dell'avviso. Il pannello dei dettagli dell'avviso fornisce ulteriori dettagli sull'avviso, tra cui un *Riepilogo*, una sezione *Prestazioni* che mostra grafici relativi ai dati dell'oggetto, eventuali *Risorse correlate* e *Commenti* inseriti dagli investigatori dell'avviso.



Avvisi quando mancano dati

In un sistema in tempo reale come Data Infrastructure Insights, per avviare l'analisi di un Monitor e decidere se generare un Alert, ci affidiamo a uno di questi due fattori:

- il prossimo punto dati ad arrivare
- un timer da attivare quando non c'è alcun punto dati e hai atteso abbastanza a lungo

Come nel caso di un arrivo lento dei dati, o di nessun arrivo dei dati, il meccanismo del timer deve subentrare poiché la velocità di arrivo dei dati non è sufficiente per attivare gli avvisi in "tempo reale". Quindi la domanda in genere diventa: "Quanto tempo devo aspettare prima di chiudere la finestra di analisi e guardare cosa ho?" Se aspetti troppo a lungo, gli avvisi non verranno generati abbastanza velocemente da risultare utili.

Se si dispone di un Monitor con una finestra di 30 minuti che rileva che una condizione è stata violata dall'ultimo punto dati prima di una perdita di dati a lungo termine, verrà generato un avviso perché il Monitor

non ha ricevuto altre informazioni da utilizzare per confermare il ripristino della metrica o per rilevare che la condizione persiste.

Avvisi "Permanentemente attivi"

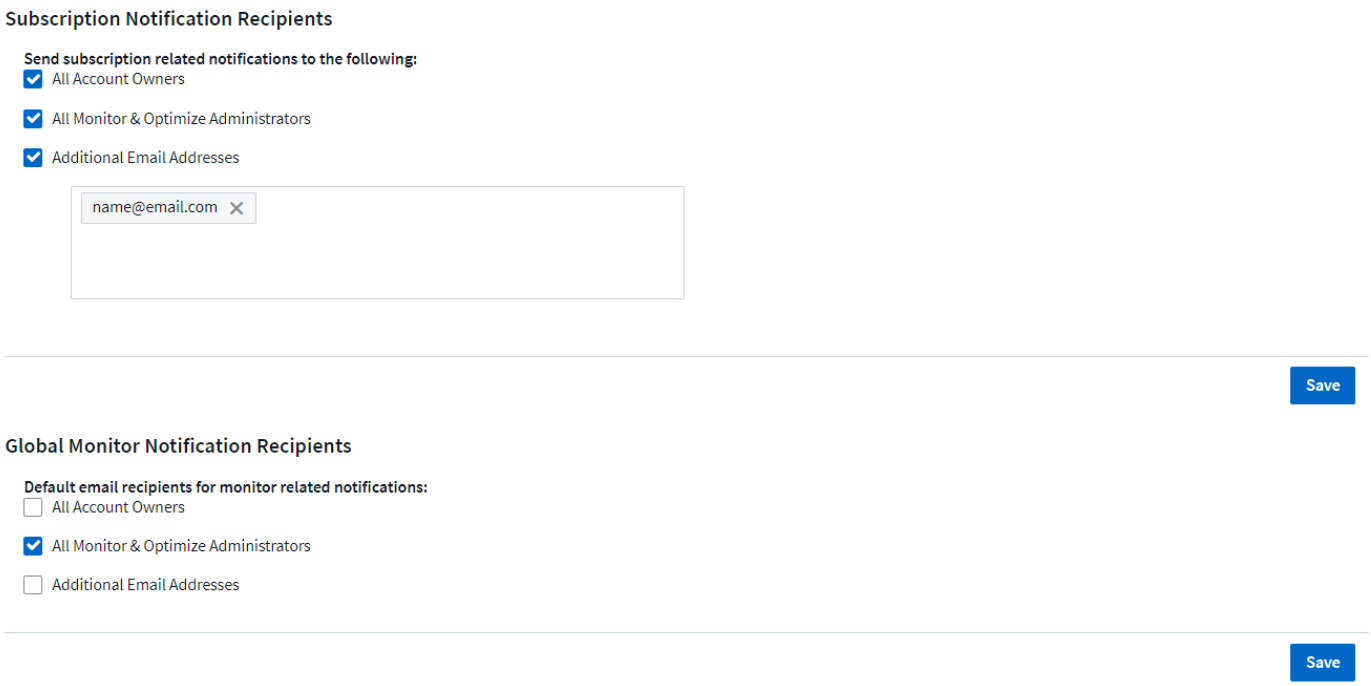
È possibile configurare un monitor in modo che la condizione sia **sempre** presente sull'oggetto monitorato, ad esempio IOPS > 1 o latenza > 0. Spesso vengono creati come monitor "di prova" e poi dimenticati. Tali monitor creano avvisi che rimangono costantemente aperti sugli oggetti costituenti, il che può causare stress al sistema e problemi di stabilità nel tempo.

Per evitare ciò, Data Infrastructure Insights chiuderà automaticamente tutti gli avvisi "permanentemente attivi" dopo 7 giorni. Si noti che le condizioni di monitoraggio sottostanti potrebbero (probabilmente) continuare a sussistere, causando l'emissione quasi immediata di un nuovo avviso, ma questa chiusura degli avvisi "sempre attivi" allevia parte dello stress del sistema che potrebbe altrimenti verificarsi.

Configurazione delle notifiche e-mail

È possibile configurare un elenco di posta elettronica per le notifiche relative agli abbonamenti, nonché un elenco di posta elettronica globale di destinatari per la notifica delle violazioni delle soglie dei criteri di prestazione.

Per configurare le impostazioni del destinatario delle notifiche via e-mail, vai alla pagina **Amministrazione > Notifiche** e seleziona la scheda *E-mail*.



Destinatari della notifica di abbonamento

Per configurare i destinatari delle notifiche degli eventi relativi all'abbonamento, vai alla sezione "Destinatari delle notifiche di abbonamento". Puoi scegliere di inviare notifiche e-mail per gli eventi relativi all'abbonamento a uno o a tutti i seguenti destinatari:

- Tutti i titolari di account
- Tutti gli amministratori di *Monitor & Optimize*

- Indirizzi email aggiuntivi che specifichi

Di seguito sono riportati alcuni esempi dei tipi di notifiche che potrebbero essere inviate e delle azioni che l'utente può intraprendere.

Notifica:	Azione dell'utente:
La versione di prova o l'abbonamento sono stati aggiornati	Rivedi i dettagli dell'abbonamento su"Sottoscrizione" pagina
L'abbonamento scadrà tra 90 giorni L'abbonamento scadrà tra 30 giorni	Nessuna azione necessaria se è abilitato il "Rinnovo automatico". Contattare il reparto vendite NetApp per rinnovare l'abbonamento.
Il processo termina tra 2 giorni	Rinnova la prova dal"Sottoscrizione" pagina. È possibile rinnovare la prova una sola volta. Contatta il reparto vendite NetApp per acquistare un abbonamento
La prova o l'abbonamento sono scaduti. L'account smetterà di raccogliere dati tra 48 ore. L'account verrà eliminato dopo 48 ore.	Contatta il reparto vendite NetApp per acquistare un abbonamento

Per assicurarti che i tuoi destinatari ricevano notifiche da Data Infrastructure Insights, aggiungi i seguenti indirizzi email a tutti gli elenchi "consentiti":

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Elenco globale dei destinatari per gli avvisi

Le notifiche e-mail degli avvisi vengono inviate all'elenco dei destinatari degli avvisi per ogni azione sull'avviso. È possibile scegliere di inviare notifiche di avviso a un elenco di destinatari globale.

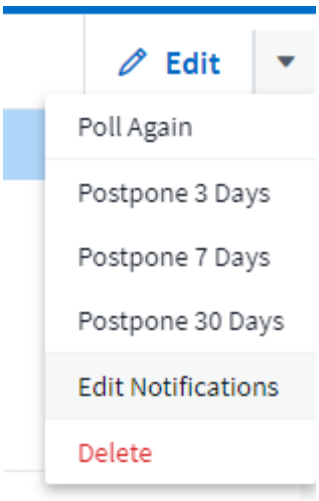
Per configurare i destinatari degli avvisi globali, selezionare i destinatari desiderati nella sezione **Destinatari delle notifiche di Global Monitor**.

È sempre possibile sovrascrivere l'elenco dei destinatari globali per un singolo monitor durante la creazione o la modifica del monitor.

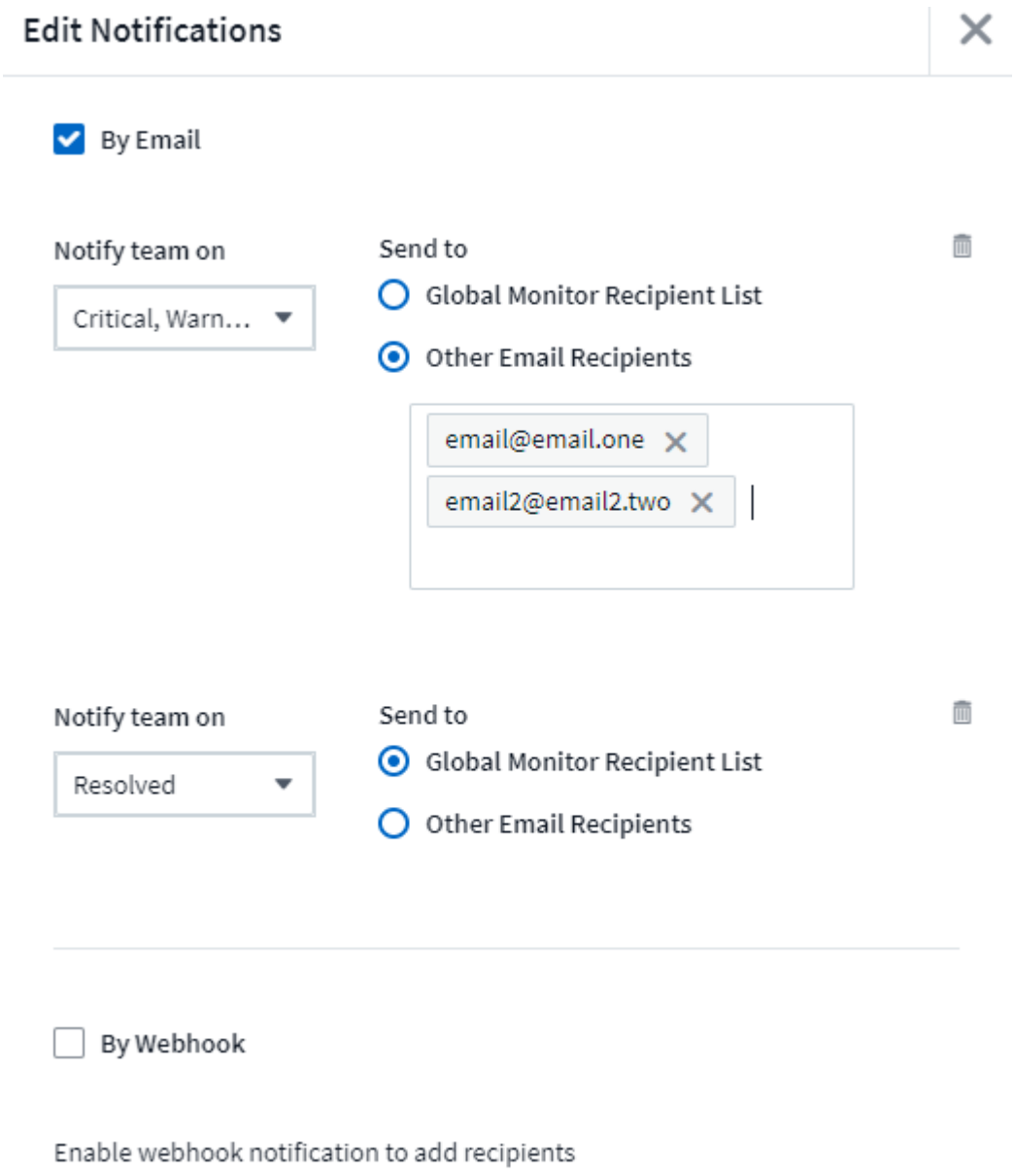
Le notifiche di ONTAP Data Collector hanno la precedenza su qualsiasi notifica specifica di Monitor pertinente al cluster/data collector. L'elenco dei destinatari impostato per il Data Collector riceverà gli avvisi del Data Collector. Se non sono presenti avvisi attivi del raccoglitore dati, gli avvisi generati dal monitor verranno inviati a destinatari specifici del monitor.

Modifica delle notifiche per ONTAP

È possibile modificare le notifiche per i cluster ONTAP selezionando *Modifica notifiche* dal menu a discesa in alto a destra nella landing page di Storage.



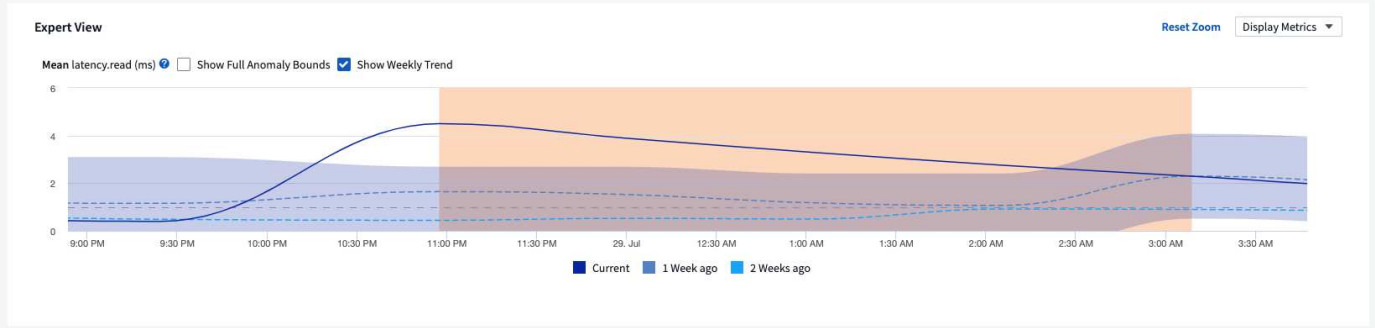
Da qui puoi impostare le notifiche per avvisi critici, di avviso, informativi e/o risolti. Ogni scenario può inviare notifiche all'elenco dei destinatari globali o ad altri destinatari scelti da te.



Monitor di rilevamento delle anomalie

Il rilevamento delle anomalie fornisce informazioni su cambiamenti imprevisti nei modelli di dati del tenant. Un'anomalia si verifica quando cambia il modello di comportamento di un oggetto, ad esempio se un oggetto presenta un certo livello di latenza a un certo orario di mercoledì, ma la latenza supera quel livello a quell'orario del mercoledì successivo, tale picco verrà considerato un'anomalia. Data Infrastructure Insights consente di creare monitor per avvisare quando si verificano anomalie di questo tipo.

Il rilevamento delle anomalie è adatto per metriche di oggetti che presentano uno schema ricorrente e prevedibile. Quando queste metriche degli oggetti superano o scendono al di sotto dei livelli previsti, Data Infrastructure Insights può generare un avviso per sollecitare un'indagine.



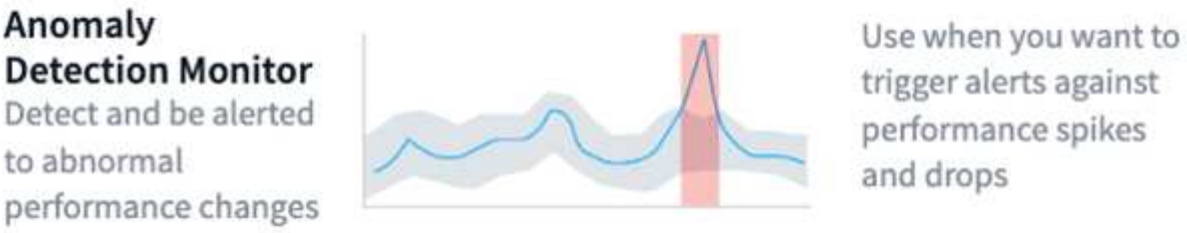
Che cos'è il rilevamento delle anomalie?

Si verifica un'anomalia quando il valore medio di una metrica si discosta di un certo numero di deviazioni standard dalla media ponderata di tale metrica per le settimane precedenti, con le settimane recenti che hanno un peso maggiore rispetto alle settimane precedenti. Data Infrastructure Insights offre la possibilità di monitorare i dati e di inviare avvisi quando vengono rilevate anomalie. È possibile impostare i livelli di "sensibilità" del rilevamento. Ad esempio, una sensibilità maggiore si avrebbe quando il valore medio si discosta dalla media con meno deviazioni standard, determinando così la generazione di più avvisi. Al contrario, minore sensibilità = più deviazioni standard dalla media = meno avvisi.

Il monitoraggio del rilevamento delle anomalie è diverso dal monitoraggio delle soglie.

- Il **monitoraggio basato su soglie** funziona quando si hanno soglie predefinite per metriche specifiche. In altre parole, quando si ha una chiara comprensione di cosa ci si aspetta (ovvero entro un intervallo normale).

- Il **monitoraggio tramite rilevamento delle anomalie** utilizza algoritmi di apprendimento automatico per identificare i valori anomali che si discostano dalla norma, quando la definizione di "normale" non è chiara.



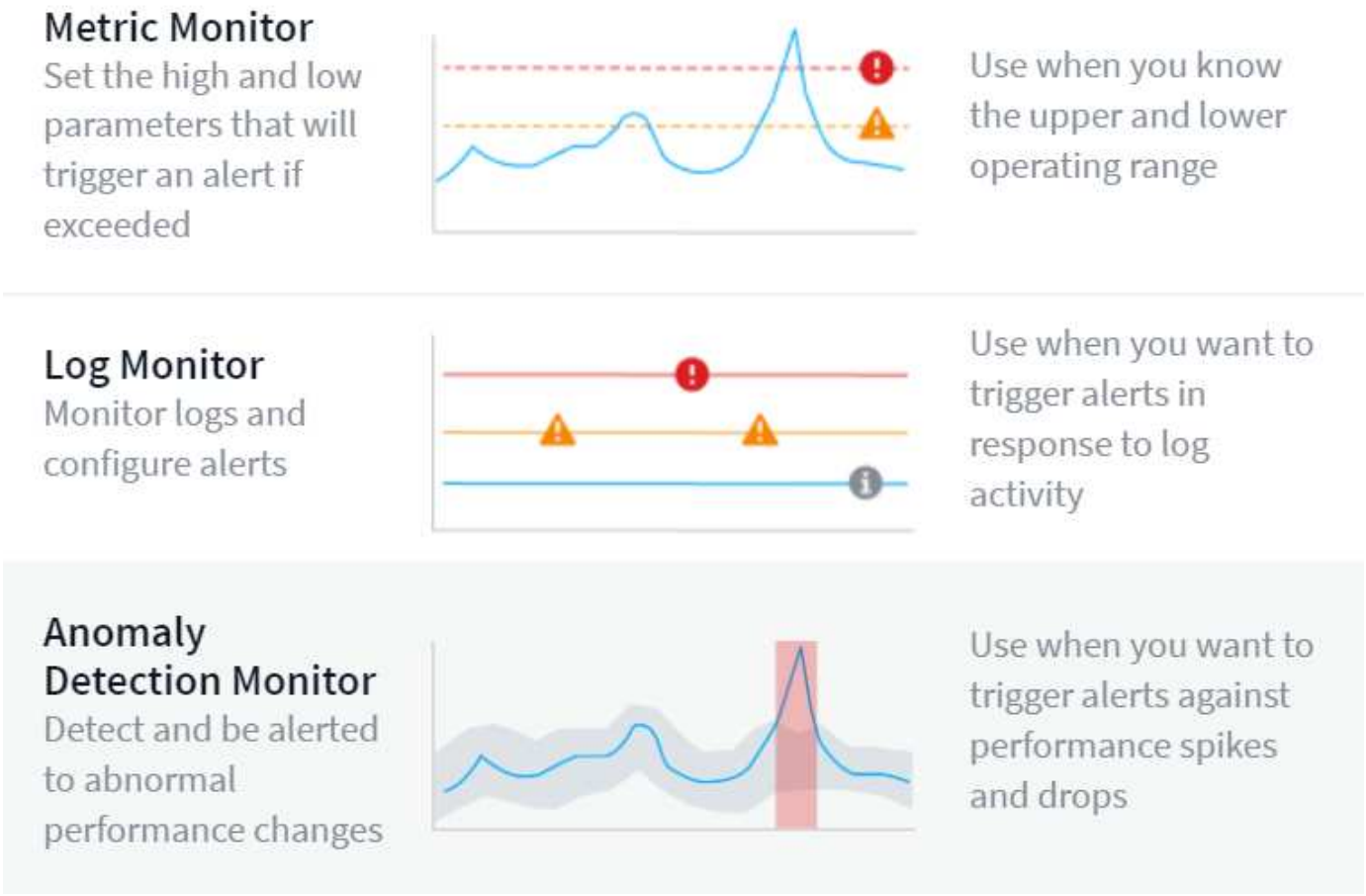
Quando avrei bisogno del rilevamento delle anomalie?

Il monitoraggio del rilevamento delle anomalie può fornire avvisi utili in molte situazioni, tra cui:

- Quando la definizione di *normale* non è chiara. Ad esempio, è possibile che i tassi di errore SAN varino a seconda della porta. Segnalare un errore è rumoroso e superfluo, ma un aumento improvviso o significativo potrebbe indicare un problema diffuso.
- Dove si verificano cambiamenti nel tempo. Carichi di lavoro che presentano stagionalità (ad esempio, sono intensi o silenziosi in determinati periodi). Ciò potrebbe includere periodi di silenzio inaspettati che potrebbero indicare un blocco del lotto.
- Lavorare con grandi quantità di dati in cui definire e regolare manualmente le soglie risulta poco pratico. Ad esempio, un tenant con un numero elevato di host e/o volumi con carichi di lavoro variabili. Ognuno di essi può avere SLA diversi, quindi è importante capire quali sono quelli che superano la norma.

Creazione di un monitor di rilevamento delle anomalie

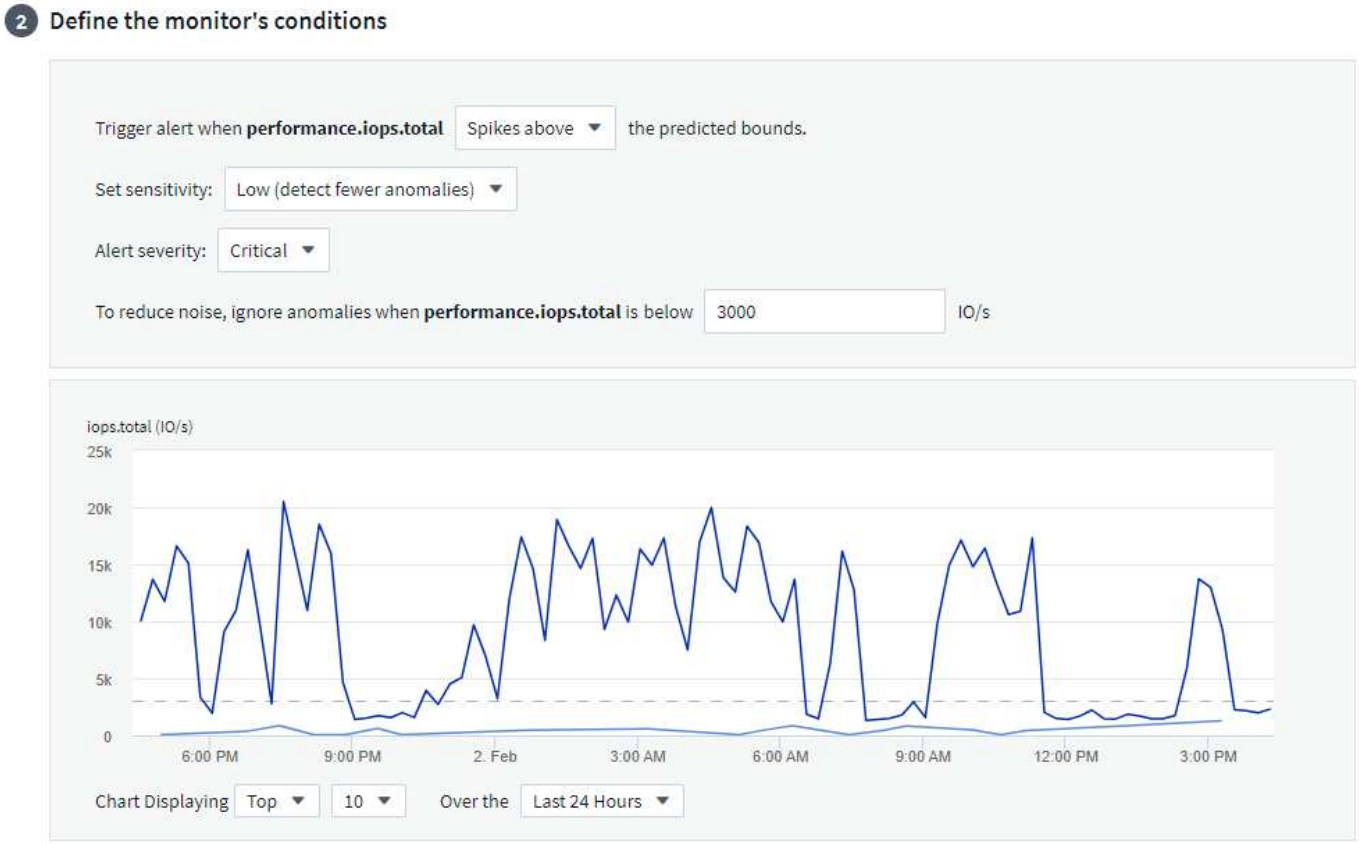
Per ricevere avvisi sulle anomalie, creare un monitor andando su **Osservabilità > Avvisi > +Monitor**. Selezionare *Anomaly Detection Monitor* come tipo di monitor.



Scegli l'oggetto e la metrica che vuoi monitorare. È possibile impostare filtri e raggruppamenti come con altri tipi di monitor.

Successivamente, impostare le condizioni per il monitor.

- Attiva un avviso quando la metrica selezionata *Raggiunge un picco* oltre i limiti previsti, *Scende al di sotto* di tali limiti o entrambe le cose.
- Impostare la sensibilità su *Media*, *Bassa* (vengono rilevate meno anomalie) o *Alta* (vengono rilevate più anomalie).
- Determina se il livello di allerta è *Critico* o *Avviso*.
- Facoltativamente, imposta un valore al di sotto del quale le anomalie vengono *ignorate*. Ciò può contribuire a ridurre il rumore. Questo valore è mostrato come una linea tratteggiata nel grafico di esempio.



Infine, è possibile configurare un metodo di recapito per gli avvisi (e-mail, webhook o entrambi), fornire al monitor una descrizione facoltativa o azioni correttive e aggiungere il monitor a un gruppo personalizzato, se lo si desidera.

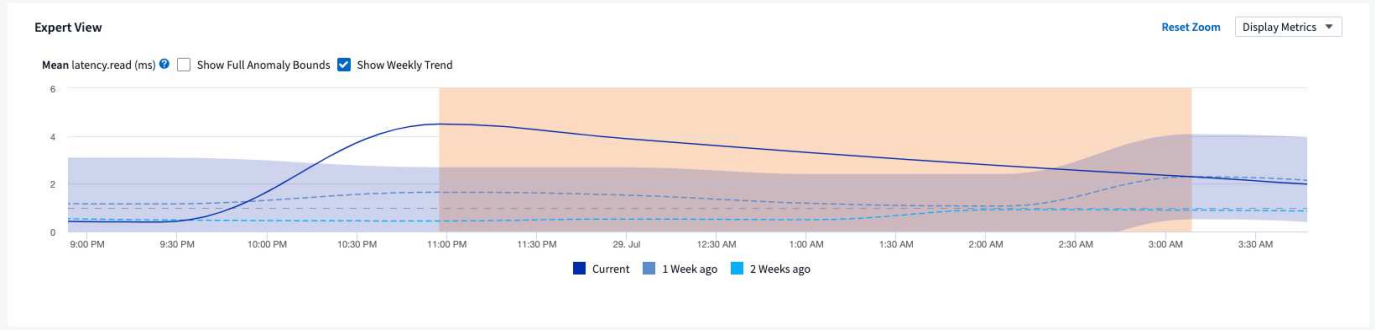
Salva il monitor con un nome significativo e il gioco è fatto.

Dopo la creazione, il monitor analizza i dati della settimana precedente per stabilire una base di riferimento iniziale. Il rilevamento delle anomalie diventa più accurato con il passare del tempo e con l'aumentare della cronologia.

> Quando viene creato un monitor, DII esamina tutti i dati esistenti della settimana precedente per individuare picchi o cali significativi; questi sono considerati anomalie. Durante la prima settimana successiva alla creazione del monitor (fase di "apprendimento"), è possibile che si verifichi un aumento del "rumore" negli avvisi. Per attenuare questo rumore, solo i picchi o i cali che durano più di 30 minuti vengono considerati anomalie e generano avvisi. Nella settimana successiva, man mano che vengono analizzati più dati, il rumore solitamente si riduce e un picco o un calo significativo che duri un certo periodo di tempo viene considerato un'anomalia.

Visualizzazione delle anomalie

Nella landing page di un avviso, gli avvisi attivati quando vengono rilevate anomalie mostreranno una banda evidenziata nel grafico, dal momento in cui la metrica ha raggiunto un picco al di fuori dei limiti previsti fino a quando è tornata all'interno di tali limiti.



Durante la visualizzazione di un grafico delle anomalie nella landing page di un avviso, è possibile scegliere le seguenti opzioni:

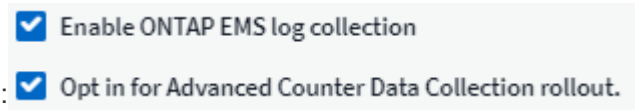
- Andamento settimanale: confronta i valori con la stessa ora, lo stesso giorno delle settimane precedenti, per un massimo di 5 settimane.
- Limiti di anomalia completi: per impostazione predefinita, il grafico si concentra sul valore della metrica, in modo da poterne analizzare meglio il comportamento. Selezionare per visualizzare i limiti completi delle anomalie (valore massimo, ecc.)

È anche possibile visualizzare gli oggetti che hanno contribuito all'anomalia selezionandoli nella sezione prestazioni della landing page. Il grafico mostrerà il comportamento degli oggetti selezionati.

Monitor di sistema

Data Infrastructure Insights include una serie di monitor definiti dal sistema sia per le metriche che per i log. I monitor di sistema disponibili dipendono dai collettori di dati presenti sul tenant. Per questo motivo, i monitor disponibili in Data Infrastructure Insights potrebbero cambiare man mano che vengono aggiunti raccoglitori di dati o ne vengono modificate le configurazioni.

Per impostazione predefinita, molti monitor di sistema sono in stato *In pausa*. È possibile abilitare un monitor di sistema selezionando l'opzione *Riprendi* per il monitor. Assicurarsi che le opzioni *Raccolta dati contatore avanzata* e *Abilita raccolta log ONTAP EMS* siano abilitate nel Data Collector. Queste opzioni sono disponibili in ONTAP Data Collector in *Configurazione avanzata*:



indice:[]

Descrizioni del monitor

I monitor definiti dal sistema sono composti da metriche e condizioni predefinite, nonché da descrizioni predefinite e azioni correttive, che non possono essere modificate. È possibile modificare l'elenco dei destinatari delle notifiche per i monitor definiti dal sistema. Per visualizzare le metriche, le condizioni, la descrizione e le azioni correttive, oppure per modificare l'elenco dei destinatari, aprire un gruppo di monitor definito dal sistema e fare clic sul nome del monitor nell'elenco.

I gruppi di monitor definiti dal sistema non possono essere modificati o rimossi.

Sono disponibili i seguenti monitor definiti dal sistema, nei gruppi indicati.

- * ONTAP Infrastructure* include monitor per problemi relativi all'infrastruttura nei cluster ONTAP .
- * Esempi di carico di lavoro ONTAP * include monitor per problemi correlati al carico di lavoro.
- Per impostazione predefinita, i monitor di entrambi i gruppi sono impostati sullo stato *Paused*.

Di seguito sono elencati i monitor di sistema attualmente inclusi in Data Infrastructure Insights:

Monitor metrici

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva

Elevato utilizzo delle porte Fibre Channel	CRITICO	Le porte Fibre Channel Protocol vengono utilizzate per ricevere e trasferire il traffico SAN tra il sistema host del cliente e le LUN ONTAP . Se l'utilizzo delle porte è elevato, questo diventerà un collo di bottiglia e influirà in ultima analisi sulle prestazioni dei carichi di lavoro sensibili del protocollo Fibre Channel. Un avviso di avvertimento indica che è necessario adottare misure pianificate per bilanciare il traffico di rete. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per bilanciare il traffico di rete e garantire la continuità del servizio.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare i carichi di lavoro su un'altra porta FCP meno utilizzata. 2. Limitare il traffico di determinate LUN solo al lavoro essenziale, tramite policy QoS in ONTAP o configurazione lato host per alleggerire l'utilizzo delle porte FCP. Se la soglia di allerta viene superata, pianificare le seguenti azioni: 1. Configurare più porte FCP per gestire il traffico dati in modo che l'utilizzo delle porte venga distribuito tra più porte. 2. Spostare i carichi di lavoro su un'altra porta FCP meno utilizzata. 3. Limitare il traffico di determinate LUN solo al lavoro essenziale, tramite policy QoS in ONTAP o configurazione lato host per alleggerire l'utilizzo delle porte FCP.

Latenza LUN elevata	CRITICO	Le LUN sono oggetti che gestiscono il traffico I/O, spesso gestito da applicazioni sensibili alle prestazioni, come i database. Le latenze LUN elevate comportano che le applicazioni stesse potrebbero risentirne e non essere in grado di svolgere le proprie attività. Un avviso di avvertimento indica che è necessario intraprendere un'azione pianificata per spostare la LUN sul nodo o sull'aggregato appropriato. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per garantire la continuità del servizio. Di seguito sono riportate le latenze previste in base al tipo di supporto: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi	Se viene superata la soglia critica, prendere in considerazione le seguenti azioni per ridurre al minimo l'interruzione del servizio: se alla LUN o al suo volume è associata una policy QoS, valutare i limiti di soglia e verificare se stanno causando la limitazione del carico di lavoro della LUN. Se la soglia di allerta viene superata, pianificare le seguenti azioni: 1. Se anche l'aggregato è sottoposto a un utilizzo elevato, spostare la LUN su un altro aggregato. 2. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo. 3. Se alla LUN o al suo volume è associata una policy QoS, valutare i limiti di soglia e verificare se stanno causando la limitazione del carico di lavoro della LUN.

Utilizzo elevato delle porte di rete	CRITICO	Le porte di rete vengono utilizzate per ricevere e trasferire il traffico dei protocolli NFS, CIFS e iSCSI tra i sistemi host del cliente e i volumi ONTAP . Se l'utilizzo delle porte è elevato, si crea un collo di bottiglia e in ultima analisi influirà sulle prestazioni dei carichi di lavoro NFS, CIFS e iSCSI. Un avviso di avviso indica che è necessario adottare misure pianificate per bilanciare il traffico di rete. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per bilanciare il traffico di rete e garantire la continuità del servizio.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Limitare il traffico di determinati volumi solo al lavoro essenziale, tramite policy QoS in ONTAP o analisi lato host per ridurre l'utilizzo delle porte di rete. 2. Configurare uno o più volumi per utilizzare un'altra porta di rete meno utilizzata. Se la soglia di allerta viene superata, prendere in considerazione le seguenti azioni immediate: 1. Configurare più porte di rete per gestire il traffico dati in modo che l'utilizzo delle porte venga distribuito tra più porte. 2. Configurare uno o più volumi per utilizzare un'altra porta di rete meno utilizzata.

Latenza elevata dello spazio dei nomi NVMe	CRITICO	Gli spazi dei nomi NVMe sono oggetti che gestiscono il traffico I/O gestito da applicazioni sensibili alle prestazioni, come i database. Un'elevata latenza degli spazi dei nomi NVMe significa che le applicazioni stesse potrebbero risentirne e non essere in grado di svolgere le proprie attività. Un avviso di avviso indica che è necessario intraprendere un'azione pianificata per spostare la LUN sul nodo o sull'aggregato appropriato. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per garantire la continuità del servizio.	Se viene superata la soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: se allo spazio dei nomi NVMe o al suo volume è assegnata una policy QoS, valutare le relative soglie limite nel caso in cui stiano causando la limitazione del carico di lavoro dello spazio dei nomi NVMe. Se la soglia di avviso viene superata, valutare di adottare le seguenti misure: 1. Se anche l'aggregato è sottoposto a un utilizzo elevato, spostare la LUN su un altro aggregato. 2. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo. 3. Se allo spazio dei nomi NVMe o al suo volume è assegnata una policy QoS, valutare le relative soglie limite nel caso in cui causino la limitazione del carico di lavoro dello spazio dei nomi NVMe.

Capacità QTree piena	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota di spazio predefinita o una quota definita da una politica di quota per limitare la quantità di dati archiviati nell'albero entro la capacità del volume. Un avviso di avviso indica che è necessario intraprendere un'azione pianificata per aumentare lo spazio. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per liberare spazio e garantire la continuità del servizio.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del qtree per assecondare la crescita. 2. Elimina i dati indesiderati per liberare spazio. Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare lo spazio del qtree per assecondare la crescita. 2. Elimina i dati indesiderati per liberare spazio.
Limite massimo di capacità QTree	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota di spazio misurata in KByte che viene utilizzata per archiviare i dati in modo da controllare la crescita del volume dei dati dell'utente e non superare la sua capacità totale. Un qtree mantiene una quota di capacità di archiviazione flessibile che avvisa l'utente in modo proattivo prima che raggiunga il limite della quota di capacità totale nel qtree e non sia più in grado di archiviare i dati. Il monitoraggio della quantità di dati archiviati in un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare la quota di spazio dell'albero per far fronte alla crescita 2. Chiedere all'utente di eliminare i dati indesiderati nell'albero per liberare spazio

Limite flessibile della capacità di QTree	AVVERTIMENTO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota di spazio misurata in KByte che può utilizzare per archiviare i dati, in modo da controllare la crescita del volume dei dati dell'utente e non superare la sua capacità totale. Un qtree mantiene una quota di capacità di archiviazione flessibile che avvisa l'utente in modo proattivo prima che raggiunga il limite della quota di capacità totale nel qtree e non sia più in grado di archiviare i dati. Il monitoraggio della quantità di dati archiviati in un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se la soglia di allerta viene superata, prendere in considerazione le seguenti azioni immediate: 1. Aumentare la quota di spazio per gli alberi per far fronte alla crescita. 2. Chiedere all'utente di eliminare i dati indesiderati nell'albero per liberare spazio.
Limite massimo dei file QTree	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota del numero di file che può contenere per mantenere una dimensione gestibile del file system all'interno del volume. Un qtree mantiene una quota fissa del numero di file oltre la quale i nuovi file nell'albero vengono negati. Il monitoraggio del numero di file all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare la quota del numero di file per qtree. 2. Eliminare i file indesiderati dal file system qtree.

Limite flessibile dei file QTree	AVVERTIMENTO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota del numero di file che può contenere per mantenere una dimensione gestibile del file system all'interno del volume. Un qtree mantiene una quota flessibile del numero di file per avvisare l'utente in modo proattivo prima che raggiunga il limite di file nel qtree e non sia più possibile archiviare file aggiuntivi. Il monitoraggio del numero di file all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare la quota del numero di file per qtree. 2. Eliminare i file indesiderati dal file system qtree.

Istantanea Riserva Spazio Pieno	CRITICO	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Una parte di questo spazio, denominato spazio riservato agli snapshot, viene utilizzata per archiviare gli snapshot che consentono di proteggere i dati a livello locale. Maggiore è la quantità di dati nuovi e aggiornati archiviati nel volume ONTAP , maggiore è la capacità di snapshot utilizzata e minore è la capacità di archiviazione snapshot disponibile per futuri dati nuovi o aggiornati. Se la capacità dei dati snapshot all'interno di un volume raggiunge lo spazio di riserva totale per gli snapshot, il cliente potrebbe non essere in grado di archiviare nuovi dati snapshot e il livello di protezione dei dati nel volume potrebbe ridursi. Il monitoraggio della capacità snapshot del volume utilizzato garantisce la continuità dei servizi dati.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena. 2. Elimina alcuni vecchi snapshot indesiderati per liberare spazio. Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare lo spazio di riserva degli snapshot all'interno del volume per adattarsi alla crescita. 2. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena.

Limite di capacità di archiviazione	CRITICO	Quando un pool di archiviazione (aggregato) si riempie, le operazioni di I/O rallentano e infine si interrompono, causando un'interruzione dell'archiviazione. Un avviso di avviso indica che è necessario intraprendere al più presto un'azione pianificata per ripristinare lo spazio libero minimo. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per liberare spazio e garantire la continuità del servizio.	Se viene superata la soglia critica, prendere immediatamente in considerazione le seguenti azioni per ridurre al minimo l'interruzione del servizio: 1. Eliminare gli snapshot sui volumi non critici. 2. Eliminare volumi o LUN che rappresentano carichi di lavoro non essenziali e che possono essere ripristinati da copie esterne all'archiviazione. Se la soglia di avviso viene superata, pianificare le seguenti azioni immediate: 1. Spostare uno o più volumi in una posizione di archiviazione diversa. 2. Aggiungere più capacità di archiviazione. 3. Modifica le impostazioni di efficienza dell'archiviazione o sposta i dati inattivi nell'archiviazione cloud.

Limite delle prestazioni di archiviazione	CRITICO	Quando un sistema di storage raggiunge il limite delle prestazioni, le operazioni rallentano, la latenza aumenta e i carichi di lavoro e le applicazioni potrebbero iniziare a non funzionare. ONTAP valuta l'utilizzo del pool di archiviazione per i carichi di lavoro e stima la percentuale di prestazioni consumata. Un avviso di avviso indica che è necessario intraprendere un'azione pianificata per ridurre il carico del pool di archiviazione e garantire che siano rimaste prestazioni sufficienti per gestire i picchi di carico di lavoro. Un avviso critico indica che è imminente un calo delle prestazioni e che è necessario adottare misure di emergenza per ridurre il carico del pool di archiviazione e garantire la continuità del servizio.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Sospendere le attività pianificate come gli snapshot o la replica SnapMirror . 2. Carichi di lavoro inattivi non essenziali.… Se la soglia di allerta viene superata, adottare immediatamente le seguenti misure: 1. Spostare uno o più carichi di lavoro in una posizione di archiviazione diversa. 2. Aggiungere più nodi di archiviazione (AFF) o ripiani di dischi (FAS) e ridistribuire i carichi di lavoro 3. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione).

Limite massimo della capacità della quota utente	CRITICO	ONTAP riconosce gli utenti dei sistemi Unix o Windows che hanno i diritti di accesso ai volumi, ai file o alle directory all'interno di un volume. Di conseguenza, ONTAP consente ai clienti di configurare la capacità di archiviazione per i propri utenti o gruppi di utenti dei propri sistemi Linux o Windows. La quota dei criteri utente o di gruppo limita la quantità di spazio che l'utente può utilizzare per i propri dati. Un limite rigido di questa quota consente di notificare all'utente quando la quantità di capacità utilizzata all'interno del volume è appena prima di raggiungere la quota di capacità totale. Il monitoraggio della quantità di dati archiviati all'interno di una quota utente o di un gruppo garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio della quota utente o del gruppo per far fronte alla crescita. 2. Chiedere all'utente o al gruppo di eliminare i dati indesiderati per liberare spazio.

Limite flessibile della capacità della quota utente	AVVERTIMENTO	ONTAP riconosce gli utenti dei sistemi Unix o Windows che hanno i diritti di accesso ai volumi, ai file o alle directory all'interno di un volume. Di conseguenza, ONTAP consente ai clienti di configurare la capacità di archiviazione per i propri utenti o gruppi di utenti dei propri sistemi Linux o Windows. La quota dei criteri utente o di gruppo limita la quantità di spazio che l'utente può utilizzare per i propri dati. Un limite flessibile di questa quota consente di inviare notifiche proattive all'utente quando la quantità di capacità utilizzata all'interno del volume raggiunge la quota di capacità totale. Il monitoraggio della quantità di dati archiviati all'interno di una quota utente o di un gruppo garantisce che l'utente riceva un servizio dati ininterrotto.	Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare lo spazio della quota utente o del gruppo per far fronte alla crescita. 2. Elimina i dati indesiderati per liberare spazio.

Capacità del volume completa	CRITICO	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Maggiore è la quantità di dati memorizzati nel volume ONTAP , minore sarà la disponibilità di spazio di archiviazione per i dati futuri. Se la capacità di archiviazione dati all'interno di un volume raggiunge la capacità di archiviazione totale, il cliente potrebbe non essere in grado di archiviare i dati a causa della mancanza di capacità di archiviazione. Il monitoraggio del volume di capacità di archiviazione utilizzato garantisce la continuità dei servizi dati.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del volume per assecondare la crescita. 2. Elimina i dati indesiderati per liberare spazio. 3. Se le copie snapshot occupano più spazio della riserva snapshot, eliminare i vecchi snapshot o abilitare l'eliminazione automatica degli snapshot del volume. Se la soglia di avviso viene superata, pianificare di intraprendere le seguenti azioni immediate: 1. Aumentare lo spazio del volume per accogliere la crescita 2. Se le copie degli snapshot occupano più spazio della riserva di snapshot, eliminare i vecchi snapshot o abilitare l'eliminazione automatica degli snapshot del volume.

Limite di volume inode	CRITICO	I volumi che archiviano i file utilizzano nodi di indice (inode) per archiviare i metadati dei file. Quando un volume esaurisce la sua allocazione di inode, non è possibile aggiungervi altri file. Un avviso di avvertenza indica che è necessario intraprendere un'azione pianificata per aumentare il numero di inode disponibili. Un avviso critico indica che l'esaurimento del limite di file è imminente e che è necessario adottare misure di emergenza per liberare inode e garantire la continuità del servizio.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare il valore degli inode per il volume. Se il valore degli inode è già al valore massimo, allora bisogna dividere il volume in due o più volumi perché il file system ha superato la dimensione massima. 2. Utilizzare FlexGroup perché aiuta a gestire file system di grandi dimensioni. Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare il valore degli inode per il volume. Se il valore degli inode è già al massimo, allora bisogna dividere il volume in due o più volumi perché il file system ha superato la dimensione massima. 2. Utilizzare FlexGroup poiché aiuta ad ospitare file system di grandi dimensioni

Latenza del volume elevata	CRITICO	I volumi sono oggetti che gestiscono il traffico I/O spesso gestito da applicazioni sensibili alle prestazioni, tra cui applicazioni DevOps, directory home e database. Le latenze elevate possono comportare problemi alle applicazioni stesse, che potrebbero non essere in grado di svolgere i propri compiti. Il monitoraggio delle latenze del volume è fondamentale per mantenere prestazioni costanti delle applicazioni. Di seguito sono riportate le latenze previste in base al tipo di supporto: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui stiano causando la limitazione del carico di lavoro del volume. Se la soglia di allerta viene superata, prendere in considerazione le seguenti azioni immediate: 1. Se anche l'aggregato è molto utilizzato, spostare il volume su un altro aggregato. 2. Se al volume è assegnata una policy QoS, valutarne le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume. 3. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo.
Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva

Nodo ad alta latenza	ATTENZIONE / CRITICO	La latenza del nodo ha raggiunto livelli tali da poter influire sulle prestazioni delle applicazioni sul nodo. Una latenza dei nodi inferiore garantisce prestazioni costanti delle applicazioni. Le latenze previste in base al tipo di supporto sono: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Sospendere le attività pianificate, gli snapshot o la replica SnapMirror 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Disattivare i carichi di lavoro non essenziali. Prendere in considerazione azioni immediate quando viene superata la soglia di avviso: 1. Spostare uno o più carichi di lavoro in una posizione di archiviazione diversa 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Aggiungere più nodi di archiviazione (AFF) o ripiani di dischi (FAS) e ridistribuire i carichi di lavoro 4. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Limite delle prestazioni del nodo	ATTENZIONE / CRITICO	L'utilizzo delle prestazioni del nodo ha raggiunto livelli tali da poter influire sulle prestazioni degli I/O e delle applicazioni supportate dal nodo. Un basso utilizzo delle prestazioni dei nodi garantisce prestazioni costanti delle applicazioni.	È necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica: 1. Sospendere le attività pianificate, gli snapshot o la replica SnapMirror 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Disattivare i carichi di lavoro non essenziali. Prendere in considerazione le seguenti azioni se viene superata la soglia di avviso: 1. Spostare uno o più carichi di lavoro in una posizione di archiviazione diversa 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Aggiungere più nodi di archiviazione (AFF) o ripiani di dischi (FAS) e ridistribuire i carichi di lavoro 4. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Storage VM ad alta latenza	ATTENZIONE / CRITICO	La latenza della VM di archiviazione (SVM) ha raggiunto livelli tali da poter influire sulle prestazioni delle applicazioni sulla VM di archiviazione. La latenza ridotta delle VM di archiviazione garantisce prestazioni costanti delle applicazioni. Le latenze previste in base al tipo di supporto sono: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	Se viene superata la soglia critica, valutare immediatamente i limiti di soglia per i volumi della VM di archiviazione con una policy QoS assegnata, per verificare se stanno causando la limitazione dei carichi di lavoro del volume. Prendere in considerazione le seguenti azioni immediate quando viene superata la soglia di avviso: 1. Se anche l'aggregato è sottoposto a un utilizzo elevato, spostare alcuni volumi della VM di archiviazione su un altro aggregato. 2. Per i volumi della VM di archiviazione con una policy QoS assegnata, valutare i limiti di soglia se causano la limitazione dei carichi di lavoro del volume 3. Se il nodo è soggetto a un utilizzo elevato, spostare alcuni volumi della VM di archiviazione su un altro nodo o ridurre il carico di lavoro totale del nodo
Limite massimo dei file delle quote utente	CRITICO	Il numero di file creati nel volume ha raggiunto il limite critico e non è possibile creare file aggiuntivi. Il monitoraggio del numero di file archiviati garantisce all'utente un servizio dati ininterrotto.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica. Si consideri l'adozione delle seguenti misure: 1. Aumentare la quota del numero di file per l'utente specifico 2. Elimina i file indesiderati per ridurre la pressione sulla quota di file per l'utente specifico

Limite flessibile dei file delle quote utente	AVVERTIMENTO	Il numero di file creati all'interno del volume ha raggiunto il limite di soglia della quota ed è prossimo al limite critico. Non è possibile creare file aggiuntivi se la quota raggiunge il limite critico. Monitorando il numero di file archiviati da un utente si garantisce che l'utente riceva un servizio dati ininterrotto.	Prendere in considerazione azioni immediate se viene superata la soglia di allerta: 1. Aumentare la quota del numero di file per la quota utente specifica 2. Elimina i file indesiderati per ridurre la pressione sulla quota di file per l'utente specifico

Rapporto di mancata corrispondenza della cache del volume	ATTENZIONE / CRITICO	Il rapporto di mancata lettura nella cache del volume è la percentuale di richieste di lettura provenienti dalle applicazioni client che vengono restituite dal disco anziché dalla cache. Ciò significa che il volume ha raggiunto la soglia impostata.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Se non è già presente sul nodo del volume, aumentare la cache WAFL acquistando e aggiungendo una Flash Cache 3. Ridurre la richiesta di carichi di lavoro a priorità inferiore sullo stesso nodo tramite limiti QoS. Prendere in considerazione azioni immediate quando viene superata la soglia di avviso: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Se non è già presente sul nodo del volume, aumentare la cache WAFL acquistando e aggiungendo una Flash Cache 3. Ridurre la richiesta di carichi di lavoro con priorità inferiore sullo stesso nodo tramite limiti QoS 4. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Sovracommit della quota Qtree del volume	ATTENZIONE / CRITICO	Volume Qtree Quota Overcommit specifica la percentuale in cui un volume è considerato in eccesso rispetto alle quote qtree. È stata raggiunta la soglia impostata per la quota qtree per il volume. Il monitoraggio del superamento della quota qtree del volume garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del volume 2. Eliminare i dati indesiderati Quando viene superata la soglia di avviso, valutare l'aumento dello spazio del volume.

Torna all'inizio

Monitor di registro

Nome del monitor	Gravità	Descrizione	Azione correttiva
Credenziali AWS non inizializzate	INFORMAZIONI	Questo evento si verifica quando un modulo tenta di accedere alle credenziali basate sui ruoli di Amazon Web Services (AWS) Identity and Access Management (IAM) dal thread delle credenziali cloud prima che vengano inizializzate.	Attendi che il thread delle credenziali cloud e il sistema completino l'inizializzazione.

Livello cloud non raggiungibile	CRITICO	Un nodo di archiviazione non riesce a connettersi all'API dell'archivio oggetti Cloud Tier. Alcuni dati saranno inaccessibili.	Se si utilizzano prodotti on-premise, eseguire le seguenti azioni correttive: …Verificare che il LIF intercluster sia online e funzionante utilizzando il comando "network interface show"….Verificare la connettività di rete al server dell'archivio oggetti utilizzando il comando "ping" sul LIF intercluster del nodo di destinazione….Assicurarsi di quanto segue:…La configurazione dell'archivio oggetti non è cambiata….Le informazioni di accesso e connettività sono ancora valide….Contattare l'assistenza tecnica NetApp se il problema persiste. Se si utilizza Cloud Volumes ONTAP, eseguire le seguenti azioni correttive: …Assicurarsi che la configurazione dell'archivio oggetti non sia cambiata…. Assicurarsi che le informazioni di accesso e connettività siano ancora valide. Se il problema persiste, contattare l'assistenza tecnica NetApp .
Disco fuori servizio	INFORMAZIONI	Questo evento si verifica quando un disco viene rimosso dal servizio perché è stato contrassegnato come guasto, è in fase di sanificazione o è entrato nel Centro di manutenzione.	Nessuno.

Costituente FlexGroup completo	CRITICO	Un componente all'interno di un volume FlexGroup è pieno, il che potrebbe causare una potenziale interruzione del servizio. È ancora possibile creare o espandere file sul volume FlexGroup . Tuttavia, nessuno dei file memorizzati sul costituente può essere modificato. Di conseguenza, potrebbero verificarsi errori casuali di spazio insufficiente quando si tenta di eseguire operazioni di scrittura sul volume FlexGroup .	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -files +X". In alternativa, eliminare i file dal volume FlexGroup . Tuttavia, è difficile stabilire quali fascicoli siano stati inoltrati al costituente.
Costituente Flexgroup quasi pieno	AVVERTIMENTO	Un componente all'interno di un volume FlexGroup ha quasi esaurito lo spazio, il che potrebbe causare una potenziale interruzione del servizio. I file possono essere creati ed espansi. Tuttavia, se lo spazio disponibile sul costituente esaurisce, potresti non essere in grado di aggiungere o modificare i file sul costituente.	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -files +X". In alternativa, eliminare i file dal volume FlexGroup . Tuttavia, è difficile stabilire quali fascicoli siano stati inoltrati al costituente.
Il componente FlexGroup ha quasi esaurito gli inode	AVVERTIMENTO	Un componente all'interno di un volume FlexGroup è quasi senza inode, il che potrebbe causare una potenziale interruzione del servizio. Il costituente riceve meno richieste di creazione rispetto alla media. Ciò potrebbe avere un impatto sulle prestazioni complessive del volume FlexGroup , poiché le richieste vengono indirizzate ai componenti con più inode.	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -files +X". In alternativa, eliminare i file dal volume FlexGroup . Tuttavia, è difficile stabilire quali fascicoli siano stati inoltrati al costituente.

Costituente FlexGroup fuori dagli inode	CRITICO	Un componente di un volume FlexGroup ha esaurito gli inode, il che potrebbe causare una potenziale interruzione del servizio. Non è possibile creare nuovi file su questo costituente. Ciò potrebbe portare a una distribuzione complessivamente sbilanciata dei contenuti nel volume FlexGroup .	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -files +X". In alternativa, eliminare i file dal volume FlexGroup . Tuttavia, è difficile stabilire quali fascicoli siano stati inoltrati al costituente.
LUN offline	INFORMAZIONI	Questo evento si verifica quando una LUN viene portata offline manualmente.	Riportare online la LUN.
Ventola dell'unità principale guasta	AVVERTIMENTO	Una o più ventole dell'unità principale sono guaste. Il sistema rimane operativo. Tuttavia, se la condizione persiste troppo a lungo, la sovratemperatura potrebbe innescare uno spegnimento automatico.	Riposizionare le ventole guaste. Se l'errore persiste, sostituirli.
Ventola dell'unità principale in stato di avviso	INFORMAZIONI	Questo evento si verifica quando una o più ventole dell'unità principale sono in stato di avviso.	Sostituire le ventole indicate per evitare il surriscaldamento.

Batteria NVRAM scarica	AVVERTIMENTO	La capacità della batteria NVRAM è estremamente bassa. Potrebbe verificarsi una potenziale perdita di dati se la batteria si scarica. Il sistema genera e trasmette un messaggio AutoSupport o "call home" al supporto tecnico NetApp e alle destinazioni configurate, se configurato per farlo. La corretta consegna di un messaggio AutoSupport migliora significativamente la determinazione e la risoluzione dei problemi.	Eseguire le seguenti azioni correttive:…Visualizzare lo stato attuale della batteria, la capacità e lo stato di carica utilizzando il comando "system node environment sensors show"….Se la batteria è stata sostituita di recente o il sistema non è stato operativo per un periodo di tempo prolungato, monitorare la batteria per verificare che si stia caricando correttamente.…Contattare l'assistenza tecnica NetApp se l'autonomia della batteria continua a scendere al di sotto dei livelli critici e il sistema di storage si spegne automaticamente.
Processore di servizio non configurato	AVVERTIMENTO	Questo evento si verifica settimanalmente per ricordarti di configurare il Service Processor (SP). L' SP è un dispositivo fisico incorporato nel sistema per fornire funzionalità di accesso e gestione remota. È necessario configurare l' SP per sfruttarne tutte le funzionalità.	Eseguire le seguenti azioni correttive:…Configurare l' SP utilizzando il comando "system service-processor network modify"….Facoltativamente, ottenere l'indirizzo MAC SP utilizzando il comando "system service-processor network show"….Verificare la configurazione di rete SP utilizzando il comando "system service-processor network show"….Verificare che l' SP possa inviare un'e-mail di AutoSupport utilizzando il comando "system service-processor autosupport invoke". NOTA: gli host e i destinatari della posta elettronica AutoSupport devono essere configurati in ONTAP prima di emettere questo comando.

Processore di servizi offline	CRITICO	ONTAP non riceve più heartbeat dal Service Processor (SP), anche se sono state eseguite tutte le azioni di ripristino SP . ONTAP non può monitorare lo stato dell'hardware senza SP. …Il sistema si spegnerà per evitare danni all'hardware e perdita di dati. Imposta un avviso di panico per essere avvisato immediatamente se l' SP va offline.	Spegnere e riaccendere il sistema eseguendo le seguenti operazioni:… Estrarre il controller dallo chassis.… Reinserire il controller.… Riaccendere il controller.… Se il problema persiste, sostituire il modulo del controller.
I ventilatori dello scaffale sono guasti	CRITICO	La ventola di raffreddamento indicata o il modulo ventola dello scaffale sono guasti. I dischi nello scaffale potrebbero non ricevere un flusso d'aria di raffreddamento sufficiente, il che potrebbe causare guasti al disco.	Eseguire le seguenti azioni correttive:…Verificare che il modulo ventola sia completamente inserito e fissato. NOTA: la ventola è integrata nel modulo di alimentazione in alcuni alloggiamenti per dischi. Se il problema persiste, sostituire il modulo ventola. Se il problema persiste, contattare l'assistenza tecnica NetApp per ricevere assistenza.
Il sistema non può funzionare a causa di un guasto della ventola dell'unità principale	CRITICO	Una o più ventole dell'unità principale sono guaste, interrompendo il funzionamento del sistema. Ciò potrebbe comportare una potenziale perdita di dati.	Sostituire le ventole guaste.
Dischi non assegnati	INFORMAZIONI	Il sistema ha dischi non assegnati: la capacità viene sprecata e potrebbe essere stata applicata una configurazione errata o una modifica parziale della configurazione del sistema.	Eseguire le seguenti azioni correttive:… Determinare quali dischi non sono assegnati utilizzando il comando "disk show -n".… Assegnare i dischi a un sistema utilizzando il comando "disk assign".

Server antivirus occupato	AVVERTIMENTO	Il server antivirus è troppo occupato per accettare nuove richieste di scansione.	Se questo messaggio si verifica frequentemente, assicurarsi che siano presenti abbastanza server antivirus per gestire il carico di scansione antivirus generato dall'SVM.
Credenziali AWS per il ruolo IAM scadute	CRITICO	Cloud Volume ONTAP è diventato inaccessibile. Le credenziali basate sul ruolo Identity and Access Management (IAM) sono scadute. Le credenziali vengono acquisite dal server di metadati di Amazon Web Services (AWS) tramite il ruolo IAM e vengono utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3).	Eseguire le seguenti operazioni:…Accedere alla console di gestione AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…Verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.
Credenziali AWS per il ruolo IAM non trovate	CRITICO	Il thread delle credenziali cloud non riesce ad acquisire le credenziali basate sul ruolo di Amazon Web Services (AWS) Identity and Access Management (IAM) dal server dei metadati AWS. Le credenziali vengono utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.	Eseguire le seguenti operazioni:…Accedere alla console di gestione AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…Verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.

Credenziali AWS per il ruolo IAM non valide	CRITICO	Le credenziali basate sul ruolo Identity and Access Management (IAM) non sono valide. Le credenziali vengono acquisite dal server di metadati di Amazon Web Services (AWS) tramite il ruolo IAM e vengono utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.	Eseguire le seguenti operazioni:…Accedere alla console di gestione AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…Verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.
Ruolo AWS IAM non trovato	CRITICO	Il thread dei ruoli Identity and Access Management (IAM) non riesce a trovare un ruolo IAM di Amazon Web Services (AWS) sul server dei metadati AWS. Il ruolo IAM è necessario per acquisire le credenziali basate sul ruolo utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.	Eseguire le seguenti operazioni:…Accedere alla console di gestione AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…Verificare che il ruolo AWS IAM associato all'istanza sia valido.
Ruolo AWS IAM non valido	CRITICO	Il ruolo Amazon Web Services (AWS) Identity and Access Management (IAM) sul server metadati AWS non è valido. Cloud Volume ONTAP è diventato inaccessibile.	Eseguire le seguenti operazioni:…Accedere alla console di gestione AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…Verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.

Errore di connessione al server metadati AWS	CRITICO	Il thread dei ruoli Identity and Access Management (IAM) non riesce a stabilire un collegamento di comunicazione con il server dei metadati di Amazon Web Services (AWS). È necessario stabilire una comunicazione per acquisire le credenziali AWS IAM basate sui ruoli necessarie, utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.	Eseguire le seguenti operazioni:…Accedere alla console di gestione AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…
Limite di utilizzo dello spazio FabricPool quasi raggiunto	AVVERTIMENTO	L'utilizzo totale dello spazio FabricPool a livello di cluster da parte degli archivi di oggetti provenienti da provider con licenza di capacità ha quasi raggiunto il limite di licenza.	Eseguire le seguenti azioni correttive:…Verificare la percentuale di capacità concessa in licenza utilizzata da ciascun livello di archiviazione FabricPool utilizzando il comando "storage aggregate object-store show-space".…Eliminare le copie snapshot dai volumi con il criterio di suddivisione in livelli "snapshot" o "backup" utilizzando il comando "volume snapshot delete" per liberare spazio.…Installare una nuova licenza sul cluster per aumentare la capacità concessa in licenza.

Limite di utilizzo dello spazio FabricPool raggiunto	CRITICO	L'utilizzo totale dello spazio FabricPool a livello di cluster degli archivi di oggetti provenienti da provider con licenza di capacità ha raggiunto il limite di licenza.	Eseguire le seguenti azioni correttive:…Verificare la percentuale di capacità concessa in licenza utilizzata da ciascun livello di archiviazione FabricPool utilizzando il comando "storage aggregate object-store show-space"….Eliminare le copie snapshot dai volumi con il criterio di suddivisione in livelli "snapshot" o "backup" utilizzando il comando "volume snapshot delete" per liberare spazio.…Installare una nuova licenza sul cluster per aumentare la capacità concessa in licenza.

Restituzione dell’aggregato fallita	CRITICO	Questo evento si verifica durante la migrazione di un aggregato come parte di un giveback di failover di archiviazione (SFO), quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive:…Verificare che il LIF intercluster sia online e funzionante utilizzando il comando "network interface show"….Verificare la connettività di rete al server dell’archivio oggetti utilizzando il comando "ping" sul LIF intercluster del nodo di destinazione. …Verificare che la configurazione dell’archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette utilizzando il comando "aggregate object-store config show"….In alternativa, è possibile ignorare l’errore specificando false per il parametro "require-partner-waiting" del comando giveback.…Per ulteriori informazioni o assistenza, contattare l’assistenza tecnica NetApp .

Interconnessione HA inattiva	AVVERTIMENTO	L'interconnessione ad alta disponibilità (HA) non funziona. Rischio di interruzione del servizio quando il failover non è disponibile.	Le azioni correttive dipendono dal numero e dal tipo di collegamenti di interconnessione HA supportati dalla piattaforma, nonché dal motivo per cui l'interconnessione non funziona. …Se i collegamenti sono inattivi:…Verificare che entrambi i controller nella coppia HA siano operativi.…Per i collegamenti collegati esternamente, assicurarsi che i cavi di interconnessione siano collegati correttamente e che i moduli SFP (Small Form-Factor Pluggable), se applicabili, siano posizionati correttamente su entrambi i controller.…Per i collegamenti collegati internamente, disattivare e riattivare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link off" e "ic link on". …Se i collegamenti sono disabilitati, abilitarli utilizzando il comando "ic link on". …Se un peer non è connesso, disabilitare e riabilitare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link off" e "ic link on".…Se il problema persiste, contattare l'assistenza tecnica NetApp .

Numero massimo di sessioni per utente superato	AVVERTIMENTO	Hai superato il numero massimo di sessioni consentite per utente su una connessione TCP. Ogni richiesta di stabilire una sessione verrà respinta finché alcune sessioni non saranno rilasciate. …	Eseguire le seguenti azioni correttive: …Ispezionare tutte le applicazioni in esecuzione sul client e terminare quelle che non funzionano correttamente.…Riavviare il client.…Verificare se il problema è causato da un'applicazione nuova o esistente:…Se l'applicazione è nuova, impostare una soglia più alta per il client utilizzando il comando "cifs option modify -max-opens-same -file-per-tree". In alcuni casi i clienti funzionano come previsto, ma richiedono una soglia più alta. Dovresti avere privilegi avanzati per impostare una soglia più alta per il client. …Se il problema è causato da un'applicazione esistente, potrebbe esserci un problema con il client. Per ulteriori informazioni o assistenza, contattare l'assistenza tecnica NetApp .

Numero massimo di aperture per file superato	AVVERTIMENTO	Hai superato il numero massimo di volte in cui puoi aprire il file tramite una connessione TCP. Ogni richiesta di apertura di questo file verrà rifiutata finché non si chiudono alcune istanze aperte del file. Ciò indica in genere un comportamento anomalo dell'applicazione.	Eseguire le seguenti azioni correttive:…Ispezionare le applicazioni in esecuzione sul client utilizzando questa connessione TCP. Il client potrebbe non funzionare correttamente a causa dell'applicazione in esecuzione su di esso. Riavviare il client. Verificare se il problema è causato da un'applicazione nuova o esistente: Se l'applicazione è nuova, impostare una soglia più alta per il client utilizzando il comando "cifs option modify -max-opens-same -file-per-tree". In alcuni casi i clienti funzionano come previsto, ma richiedono una soglia più alta. Dovresti avere privilegi avanzati per impostare una soglia più alta per il client. …Se il problema è causato da un'applicazione esistente, potrebbe esserci un problema con il client. Per ulteriori informazioni o assistenza, contattare l'assistenza tecnica NetApp .

Conflitto di nomi NetBIOS	CRITICO	Il servizio nomi NetBIOS ha ricevuto una risposta negativa a una richiesta di registrazione del nome da un computer remoto. In genere ciò è causato da un conflitto nel nome NetBIOS o in un alias. Di conseguenza, i client potrebbero non essere in grado di accedere ai dati o di connettersi al nodo di distribuzione dei dati corretto nel cluster.	Eseguire una delle seguenti azioni correttive:…Se si verifica un conflitto nel nome NetBIOS o in un alias, eseguire una delle seguenti operazioni:…Eliminare l'alias NetBIOS duplicato utilizzando il comando "vserver cifs delete -aliases alias -vserver vserver".…Rinominare un alias NetBIOS eliminando il nome duplicato e aggiungendo un alias con un nuovo nome utilizzando il comando "vserver cifs create -aliases alias -vserver vserver". …Se non sono configurati alias e si verifica un conflitto nel nome NetBIOS, rinominare il server CIFS utilizzando i comandi "vserver cifs delete -vserver vserver" e "vserver cifs create -cifs -server netbiosname". NOTA: l'eliminazione di un server CIFS può rendere i dati inaccessibili. …Rimuovere il nome NetBIOS o rinominare il NetBIOS sul computer remoto.
Pool di archiviazione NFSv4 esaurito	CRITICO	Un pool di archiviazione NFSv4 è esaurito.	Se il server NFS non risponde per più di 10 minuti dopo questo evento, contattare l'assistenza tecnica NetApp .

Nessun motore di scansione registrato	CRITICO	Il connettore antivirus ha notificato a ONTAP che non dispone di un motore di scansione registrato. Ciò potrebbe causare la mancata disponibilità dei dati se è abilitata l'opzione "scan-mandatory".	Eseguire le seguenti azioni correttive:…Assicurarsi che il software del motore di scansione installato sul server antivirus sia compatibile con ONTAP.…Assicurarsi che il software del motore di scansione sia in esecuzione e configurato per connettersi al connettore antivirus tramite loopback locale.
Nessuna connessione Vscan	CRITICO	ONTAP non ha alcuna connessione Vscan per gestire le richieste di scansione antivirus. Ciò potrebbe causare la mancata disponibilità dei dati se è abilitata l'opzione "scan-mandatory".	Assicurarsi che il pool di scanner sia configurato correttamente e che i server antivirus siano attivi e connessi a ONTAP.
Spazio volume radice nodo basso	CRITICO	Il sistema ha rilevato che lo spazio disponibile nel volume root è pericolosamente basso. Il nodo non è completamente operativo. È possibile che i LIF dei dati siano falliti all'interno del cluster, per cui l'accesso NFS e CIFS è limitato sul nodo. La capacità amministrativa è limitata alle procedure di ripristino locale del nodo per liberare spazio sul volume radice.	Eseguire le seguenti azioni correttive:…Liberare spazio sul volume root eliminando le vecchie copie Snapshot, eliminando i file non più necessari dalla directory /mroot o espandendo la capacità del volume root.…Riavviare il controller.…Contattare l'assistenza tecnica NetApp per ulteriori informazioni o assistenza.
Condivisione amministratore inesistente	CRITICO	Problema Vscan: un client ha tentato di connettersi a una condivisione ONTAP_ADMIN$ inesistente.	Assicurarsi che Vscan sia abilitato per l'ID SVM menzionato. L'abilitazione di Vscan su una SVM determina la creazione automatica della condivisione ONTAP_ADMIN$ per la SVM.

Spazio dei nomi NVMe esaurito	CRITICO	Uno spazio dei nomi NVMe è stato messo offline a causa di un errore di scrittura causato dalla mancanza di spazio.	Aggiungere spazio al volume e quindi portare online lo spazio dei nomi NVMe utilizzando il comando "vserver nvme namespace modify".
Periodo di grazia NVMe-oF attivo	AVVERTIMENTO	Questo evento si verifica quotidianamente quando è in uso il protocollo NVMe over Fabrics (NVMe-oF) e il periodo di grazia della licenza è attivo. La funzionalità NVMe-oF richiede una licenza dopo la scadenza del periodo di grazia della licenza. La funzionalità NVMe-oF viene disabilitata al termine del periodo di grazia della licenza.	Contatta il tuo rappresentante di vendita per ottenere una licenza NVMe-oF e aggiungerla al cluster oppure rimuovi tutte le istanze della configurazione NVMe-oF dal cluster.
Periodo di grazia NVMe-oF scaduto	AVVERTIMENTO	Il periodo di grazia della licenza NVMe over Fabrics (NVMe-oF) è terminato e la funzionalità NVMe-oF è disabilitata.	Contatta il tuo rappresentante commerciale per ottenere una licenza NVMe-oF e aggiungerla al cluster.
Inizio del periodo di grazia NVMe-oF	AVVERTIMENTO	La configurazione NVMe over Fabrics (NVMe-oF) è stata rilevata durante l'aggiornamento al software ONTAP 9.5. La funzionalità NVMe-oF richiede una licenza dopo la scadenza del periodo di grazia della licenza.	Contatta il tuo rappresentante commerciale per ottenere una licenza NVMe-oF e aggiungerla al cluster.
Host archivio oggetti non risolvibile	CRITICO	Il nome host del server di archiviazione degli oggetti non può essere risolto in un indirizzo IP. Il client dell'archivio oggetti non può comunicare con il server dell'archivio oggetti senza risolvere un indirizzo IP. Di conseguenza, i dati potrebbero risultare inaccessibili.	Controllare la configurazione DNS per verificare che il nome host sia configurato correttamente con un indirizzo IP.

Object Store Intercluster LIF inattivo	CRITICO	Il client dell'archivio oggetti non riesce a trovare un LIF operativo per comunicare con il server dell'archivio oggetti. Il nodo non consentirà il traffico client dell'archivio oggetti finché il LIF intercluster non sarà operativo. Di conseguenza, i dati potrebbero risultare inaccessibili.	Eseguire le seguenti azioni correttive:…Verificare lo stato del LIF intercluster utilizzando il comando "network interface show -role intercluster"….Verificare che il LIF intercluster sia configurato correttamente e operativo.…Se un LIF intercluster non è configurato, aggiungerlo utilizzando il comando "network interface create -role intercluster".
Mancata corrispondenza della firma dell'archivio oggetti	CRITICO	La firma della richiesta inviata al server dell'archivio oggetti non corrisponde alla firma calcolata dal client. Di conseguenza, i dati potrebbero risultare inaccessibili.	Verificare che la chiave di accesso segreta sia configurata correttamente. Se la configurazione è corretta, contattare il supporto tecnico NetApp per ricevere assistenza.
Timeout READDIR	CRITICO	Un'operazione sul file READDIR ha superato il timeout consentito per l'esecuzione in WAFL. Ciò può essere dovuto a directory molto grandi o sparse. Si raccomanda un'azione correttiva.	Eseguire le seguenti azioni correttive:…Trovare informazioni specifiche sulle directory recenti le cui operazioni sui file READDIR sono scadute utilizzando il seguente comando CLI nodeshell con privilegio 'diag': wafl readdir notice show.…Controllare se le directory sono indicate come sparse o meno:…Se una directory è indicata come sparse, si consiglia di copiare il contenuto della directory in una nuova directory per rimuovere la scarsità del file della directory. …Se una directory non è indicata come sparse e la directory è di grandi dimensioni, si consiglia di ridurre le dimensioni del file della directory riducendo il numero di voci di file nella directory.

Trasferimento dell’aggregato non riuscito	CRITICO	Questo evento si verifica durante lo spostamento di un aggregato, quando il nodo di destinazione non riesce a raggiungere gli archivi degli oggetti.	Eseguire le seguenti azioni correttive:…Verificare che il LIF intercluster sia online e funzionante utilizzando il comando "network interface show".…Verificare la connettività di rete al server dell’archivio oggetti utilizzando il comando "ping" sul LIF intercluster del nodo di destinazione. …Verificare che la configurazione dell’archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette utilizzando il comando "aggregate object-store config show".…In alternativa, è possibile ignorare l’errore utilizzando il parametro "override-destination-checks" del comando di rilocazione.…Per ulteriori informazioni o assistenza, contattare l’assistenza tecnica NetApp .
Copia shadow non riuscita	CRITICO	Si è verificato un errore nel servizio Copia Shadow del volume (VSS), un’operazione di backup e ripristino del servizio Microsoft Server.	Verificare quanto segue utilizzando le informazioni fornite nel messaggio dell’evento:…La configurazione della copia shadow è abilitata?…Sono installate le licenze appropriate? …Su quali condivisioni viene eseguita l’operazione di copia shadow?…Il nome della condivisione è corretto?…Il percorso della condivisione esiste?…Quali sono gli stati del set di copie shadow e delle relative copie shadow?

Alimentatori dell'interruttore di archiviazione guasti	AVVERTIMENTO	Manca l'alimentatore nell'interruttore del cluster. La ridondanza è ridotta, il rischio di interruzioni in caso di ulteriori interruzioni di corrente.	Eseguire le seguenti azioni correttive:…Assicurarsi che l'alimentatore principale, che fornisce energia allo switch del cluster, sia acceso.…Assicurarsi che il cavo di alimentazione sia collegato all'alimentatore.…Contattare l'assistenza tecnica NetApp se il problema persiste.
Troppe autenticazioni CIFS	AVVERTIMENTO	Si sono verificate contemporaneamente numerose negoziazioni di autenticazione. Ci sono 256 richieste di nuove sessioni incomplete da questo client.	Indagare sul motivo per cui il client ha creato 256 o più nuove richieste di connessione. Potrebbe essere necessario contattare il fornitore del client o dell'applicazione per determinare il motivo per cui si è verificato l'errore.
Accesso utente non autorizzato alla condivisione amministratore	AVVERTIMENTO	Un client ha tentato di connettersi alla condivisione privilegiata ONTAP_ADMIN$ anche se l'utente connesso non è un utente autorizzato.	Eseguire le seguenti azioni correttive:…Assicurarsi che il nome utente e l'indirizzo IP menzionati siano configurati in uno dei pool di scanner Vscan attivi.…Controllare la configurazione del pool di scanner attualmente attivo utilizzando il comando "vserver vscan scanner pool show-active".

Virus rilevato	AVVERTIMENTO	Un server Vscan ha segnalato un errore al sistema di archiviazione. In genere questo indica che è stato trovato un virus. Tuttavia, altri errori sul server Vscan possono causare questo evento.…L'accesso del client al file è negato. A seconda delle impostazioni e della configurazione, il server Vscan potrebbe pulire il file, metterlo in quarantena o eliminarlo.	Controllare il registro del server Vscan riportato nell'evento "syslog" per verificare se è riuscito a pulire, mettere in quarantena o eliminare correttamente il file infetto. Se ciò non fosse possibile, un amministratore di sistema potrebbe dover eliminare manualmente il file.
Volume offline	INFORMAZIONI	Questo messaggio indica che un volume è stato reso offline.	Ripristinare il volume online.
Volume limitato	INFORMAZIONI	Questo evento indica che un volume flessibile è stato reso limitato.	Ripristinare il volume online.
Arresto della VM di archiviazione riuscito	INFORMAZIONI	Questo messaggio viene visualizzato quando un'operazione di 'arresto del vserver' riesce.	Utilizzare il comando 'vserver start' per avviare l'accesso ai dati su una VM di archiviazione.
Nodo Panico	AVVERTIMENTO	Questo evento viene emesso quando si verifica un panico	Contattare l'assistenza clienti NetApp .

Torna all'inizio

Monitor di registro anti-ransomware

Nome del monitor	Gravità	Descrizione	Azione correttiva
Monitoraggio anti-ransomware VM di archiviazione disabilitato	AVVERTIMENTO	Il monitoraggio anti-ransomware per la VM di archiviazione è disabilitato. Abilitare l'anti-ransomware per proteggere la VM di archiviazione.	Nessuno
Monitoraggio anti-ransomware della VM di archiviazione abilitato (modalità di apprendimento)	INFORMAZIONI	Il monitoraggio anti-ransomware per la VM di archiviazione è abilitato in modalità di apprendimento.	Nessuno

Monitoraggio anti-ransomware del volume abilitato	INFORMAZIONI	Il monitoraggio anti-ransomware per il volume è abilitato.	Nessuno
Monitoraggio anti-ransomware del volume disabilitato	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è disabilitato. Abilitare l'anti-ransomware per proteggere il volume.	Nessuno
Monitoraggio anti-ransomware del volume abilitato (modalità di apprendimento)	INFORMAZIONI	Il monitoraggio anti-ransomware per il volume è abilitato in modalità di apprendimento.	Nessuno
Monitoraggio anti-ransomware del volume sospeso (modalità di apprendimento)	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è in pausa in modalità di apprendimento.	Nessuno
Monitoraggio anti-ransomware del volume sospeso	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è sospeso.	Nessuno
Disattivazione del monitoraggio anti-ransomware del volume	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è disabilitato.	Nessuno
Attività ransomware rilevata	CRITICO	Per proteggere i dati dal ransomware rilevato, è stata creata una copia Snapshot che può essere utilizzata per ripristinare i dati originali. Il sistema genera e trasmette un messaggio AutoSupport o "chiama casa" al supporto tecnico NetApp e a tutte le destinazioni configurate. Il messaggio AutoSupport migliora la determinazione e la risoluzione dei problemi.	Fare riferimento a "FINAL-DOCUMENT-NAME" per adottare misure correttive in caso di attività ransomware.

Torna all'inizio

FSx per monitor NetApp ONTAP

Nome del monitor	Soglie	Descrizione del monitor	Azione correttiva

La capacità del volume FSx è piena	Attenzione @ > 85 %…Critico @ > 95 %	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Maggiore è la quantità di dati memorizzati nel volume ONTAP , minore sarà la disponibilità di spazio di archiviazione per i dati futuri. Se la capacità di archiviazione dati all'interno di un volume raggiunge la capacità di archiviazione totale, il cliente potrebbe non essere in grado di archiviare i dati a causa della mancanza di capacità di archiviazione. Il monitoraggio del volume di capacità di archiviazione utilizzato garantisce la continuità dei servizi dati.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Valuta l'eliminazione dei dati che non ti servono più per liberare spazio
Volume FSx ad alta latenza	Attenzione @ > 1000 µs…Critico @ > 2000 µs	I volumi sono oggetti che servono il traffico di I/O spesso gestito da applicazioni sensibili alle prestazioni, tra cui applicazioni DevOps, directory home e database. Le latenze elevate possono comportare problemi alle applicazioni stesse, che potrebbero non essere in grado di svolgere i propri compiti. Il monitoraggio delle latenze del volume è fondamentale per mantenere prestazioni costanti dell'applicazione.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui stiano causando la limitazione del carico di lavoro del volume… Pianificare di intraprendere quanto segue al più presto se la soglia di avviso viene superata:…1. Se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume.…2. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo.

Limite di inode del volume FSx	Attenzione @ > 85 %…Critico @ > 95 %	I volumi che archiviano i file utilizzano nodi di indice (inode) per archiviare i metadati dei file. Quando un volume esaurisce la sua allocazione di inode, non è possibile aggiungervi altri file. Un avviso di avviso indica che è necessario intraprendere un'azione pianificata per aumentare il numero di inode disponibili. Un avviso critico indica che l'esaurimento del limite dei file è imminente e che è necessario adottare misure di emergenza per liberare gli inode e garantire la continuità del servizio.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Si consiglia di aumentare il valore degli inode per il volume. Se il valore degli inode è già al massimo, allora prendi in considerazione la possibilità di dividere il volume in due o più volumi perché il file system ha superato la dimensione massima… Pianifica di intraprendere presto le seguenti azioni se viene superata la soglia di avviso:…1. Si consiglia di aumentare il valore degli inode per il volume. Se il valore degli inode è già al massimo, allora prendi in considerazione la suddivisione del volume in due o più volumi perché il file system è cresciuto oltre la dimensione massima
Sovracommit della quota Qtree del volume FSx	Attenzione @ > 95 %…Critico @ > 100 %	Volume Qtree Quota Overcommit specifica la percentuale in cui un volume è considerato in eccesso rispetto alle quote qtree. È stata raggiunta la soglia impostata per la quota qtree per il volume. Il monitoraggio del superamento della quota qtree del volume garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Eliminare i dati indesiderati… Quando viene superata la soglia di avviso, valutare l'aumento dello spazio del volume.

Lo spazio di riserva dello snapshot FSx è pieno	Attenzione @ > 90 %…Critico @ > 95 %	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Una parte di questo spazio, denominato spazio riservato agli snapshot, viene utilizzata per archiviare gli snapshot che consentono di proteggere i dati a livello locale. Maggiore è la quantità di dati nuovi e aggiornati memorizzati nel volume ONTAP , maggiore è la capacità di snapshot utilizzata e minore sarà la capacità di archiviazione snapshot disponibile per futuri dati nuovi o aggiornati. Se la capacità dei dati snapshot all'interno di un volume raggiunge lo spazio di riserva totale per gli snapshot, il cliente potrebbe non essere in grado di archiviare nuovi dati snapshot e il livello di protezione dei dati nel volume potrebbe ridursi. Il monitoraggio della capacità snapshot del volume utilizzato garantisce la continuità dei servizi dati.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Si consiglia di configurare gli snapshot in modo da utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena…2. Si consiglia di eliminare alcuni snapshot più vecchi che potrebbero non essere più necessari per liberare spazio… Si consiglia di intraprendere quanto segue al più presto se la soglia di avviso viene superata:…1. Valutare l'aumento dello spazio di riserva degli snapshot all'interno del volume per adattarsi alla crescita…2. Valutare la possibilità di configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena

Rapporto di mancata ricezione della cache del volume FSx	Attenzione @ > 95 %…Critico @ > 100 %	Il rapporto di mancata lettura nella cache del volume è la percentuale di richieste di lettura provenienti dalle applicazioni client che vengono restituite dal disco anziché dalla cache. Ciò significa che il volume ha raggiunto la soglia impostata.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore sullo stesso nodo tramite limiti QoS… Prendere in considerazione azioni immediate quando viene superata la soglia di avviso: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore sullo stesso nodo tramite limiti QoS 3. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Torna all'inizio

Monitor K8s

Nome del monitor	Descrizione	Azioni correttive	Gravità/Soglia

Latenza del volume persistente elevata	Le latenze elevate e persistenti possono compromettere il funzionamento delle applicazioni stesse e impedirne lo svolgimento delle attività. Il monitoraggio delle latenze persistenti dei volumi è fondamentale per mantenere prestazioni costanti delle applicazioni. Di seguito sono riportate le latenze previste in base al tipo di supporto: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	**Azioni immediate** Se viene superata la soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume. **Azioni da intraprendere al più presto** Se la soglia di allerta viene superata, pianificare le seguenti azioni immediate: 1. Se anche il pool di archiviazione è sottoposto a un utilizzo elevato, spostare il volume in un altro pool di archiviazione. 2. Se al volume è assegnata una policy QoS, valutarne le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume. 3. Se anche il controller è sottoposto a un utilizzo elevato, spostare il volume su un altro controller o ridurre il carico di lavoro totale del controller.	Attenzione @ > 6.000 µs Critico @ > 12.000 µs
Saturazione della memoria del cluster elevata	La saturazione della memoria allocabile del cluster è elevata. La saturazione della CPU del cluster viene calcolata come la somma dell'utilizzo della memoria divisa per la somma della memoria allocabile su tutti i nodi K8.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Attenzione @ > 80 % Critico @ > 90 %
Collegamento POD non riuscito	Questo avviso si verifica quando un collegamento di volume con POD non riesce.		Avvertimento

Alta velocità di ritrasmissione	Elevata velocità di ritrasmissione TCP	Verifica la congestione della rete: identifica i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware.	Attenzione @ > 10 % Critico @ > 25 %
Capacità elevata del file system del nodo	Capacità elevata del file system del nodo	- Aumentare le dimensioni dei dischi dei nodi per garantire che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre l'utilizzo dei file dell'applicazione.	Attenzione @ > 80 % Critico @ > 90 %
Jitter di rete del carico di lavoro elevato	Elevato jitter TCP (elevate variazioni di latenza/tempo di risposta)	Verificare la congestione della rete. Identificare i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware	Attenzione @ > 30 ms Critico @ > 50 ms

Throughput del volume persistente	Le soglie MBPS sui volumi persistenti possono essere utilizzate per avvisare un amministratore quando i volumi persistenti superano le aspettative di prestazioni predefinite, con un potenziale impatto su altri volumi persistenti. L'attivazione di questo monitor genererà avvisi appropriati per il tipico profilo di throughput dei volumi persistenti sugli SSD. Questo monitor coprirà tutti i volumi persistenti sul tuo tenant. I valori di soglia critici e di avviso possono essere regolati in base agli obiettivi di monitoraggio duplicando questo monitor e impostando soglie appropriate per la classe di archiviazione. Un monitor duplicato può essere ulteriormente indirizzato a un sottoinsieme dei volumi persistenti sul tenant.	**Azioni immediate** Se viene superata la soglia critica, pianificare azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Introdurre limiti QoS MBPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie. **Azioni da intraprendere a breve** Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti azioni: 1. Introdurre limiti QoS MBPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie.	Attenzione @ > 10.000 MB/s Critico @ > 15.000 MB/s
Contenitore a rischio di OOM ucciso	I limiti di memoria del contenitore sono impostati troppo bassi. Il contenitore rischia di essere espulso (Out of Memory Kill).	Aumentare i limiti di memoria del contenitore.	Attenzione @ > 95 %
Carico di lavoro ridotto	Il carico di lavoro non ha pod sani.		Critico @ < 1
Vincolo di richiesta di volume persistente non riuscito	Questo avviso si verifica quando un collegamento su un PVC non riesce.		Avvertimento
I limiti di ResourceQuota Mem stanno per essere superati	I limiti di memoria per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %
Richieste di memoria ResourceQuota in procinto di superare	Le richieste di memoria per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %

Creazione del nodo non riuscita	Non è stato possibile pianificare il nodo a causa di un errore di configurazione.	Controllare il registro eventi di Kubernetes per individuare la causa dell'errore di configurazione.	Critico
Recupero del volume persistente non riuscito	Il volume non ha superato il recupero automatico.		Attenzione @ > 0 B
Limitazione della CPU del contenitore	I limiti della CPU del contenitore sono impostati su un valore troppo basso. I processi dei contenitori vengono rallentati.	Aumentare i limiti della CPU del contenitore.	Attenzione @ > 95 % Critico @ > 98 %
Impossibile eliminare il servizio Load Balancer			Avvertimento
IOPS del volume persistente	Le soglie IOPS sui volumi persistenti possono essere utilizzate per avvisare un amministratore quando i volumi persistenti superano le aspettative di prestazioni predefinite. L'attivazione di questo monitor genererà avvisi appropriati per il tipico profilo IOPS dei volumi di persistenza. Questo monitor coprirà tutti i volumi persistenti sul tuo tenant. I valori di soglia di avviso e critici possono essere regolati in base agli obiettivi di monitoraggio duplicando questo monitor e impostando soglie appropriate per il carico di lavoro.	**Azioni immediate** Se viene superata la soglia critica, pianificare azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Introdurre limiti QoS IOPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie. **Azioni da intraprendere al più presto** Se la soglia di allerta viene superata, pianificare le seguenti azioni immediate: 1. Introdurre limiti QoS IOPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie.	Attenzione @ > 20.000 IO/s Critico @ > 25.000 IO/s
Impossibile aggiornare il servizio Load Balancer			Avvertimento
Montaggio POD non riuscito	Questo avviso si verifica quando un montaggio su un POD non riesce.		Avvertimento

Pressione PID del nodo	Gli identificatori di processo disponibili sul nodo (Linux) sono scesi al di sotto di una soglia di espulsione.	Trova e correggi i pod che generano molti processi e privano il nodo degli ID di processo disponibili. Imposta PodPidsLimit per proteggere il tuo nodo da pod o container che generano troppi processi.	Critico @ > 0
Errore di estrazione dell'immagine del pod	Kubernetes non è riuscito a estrarre l'immagine del contenitore pod.	- Assicurarsi che l'immagine del pod sia scritta correttamente nella configurazione del pod. - Controlla che il tag immagine esista nel tuo registro. - Verificare le credenziali per il registro delle immagini. - Verificare la presenza di problemi di connettività del registro. - Verificare di non superare i limiti di velocità imposti dai fornitori del registro pubblico.	Avvertimento
Lavoro in esecuzione da troppo tempo	Il lavoro è in esecuzione da troppo tempo		Attenzione @ > 1 ora Critico @ > 5 ore
Memoria del nodo elevata	L'utilizzo della memoria del nodo è elevato	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Attenzione @ > 85 % Critico @ > 90 %
I limiti della CPU di ResourceQuota stanno per essere superati	I limiti della CPU per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %
Pod Crash Loop Backoff	Pod si è bloccato e ha tentato di riavviarsi più volte.		Critico @ > 3
Nodo CPU alto	L'utilizzo della CPU del nodo è elevato.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare CPU sui nodi.	Attenzione @ > 80 % Critico @ > 90 %
Latenza di rete del carico di lavoro RTT elevata	Elevata latenza TCP RTT (tempo di andata e ritorno)	Verifica la congestione della rete ▒ Identifica i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware.	Attenzione @ > 150 ms Critico @ > 300 ms

Lavoro fallito	Il processo non è stato completato correttamente a causa di un arresto anomalo o riavvio del nodo, esaurimento delle risorse, timeout del processo o errore di pianificazione del pod.	Controllare i registri eventi di Kubernetes per individuare le cause degli errori.	Attenzione @ > 1
Volume persistente pieno in pochi giorni	Il volume persistente esaurirà lo spazio tra qualche giorno	-Aumentare le dimensioni del volume per garantire che ci sia spazio sufficiente per i file dell'applicazione. -Ridurre la quantità di dati memorizzati nelle applicazioni.	Attenzione @ < 8 giorni Critico @ < 3 giorni
Pressione della memoria del nodo	Il nodo sta esaurendo la memoria. La memoria disponibile ha raggiunto la soglia di espulsione.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Critico @ > 0
Nodo non pronto	Il nodo non è pronto da 5 minuti	Verificare che il nodo disponga di risorse sufficienti di CPU, memoria e disco. Controllare la connettività della rete del nodo. Controllare i registri eventi di Kubernetes per individuare le cause degli errori.	Critico @ < 1
Capacità di volume persistente elevata	La capacità utilizzata dal backend del volume persistente è elevata.	- Aumentare le dimensioni del volume per garantire che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre la quantità di dati memorizzati nelle applicazioni.	Attenzione @ > 80 % Critico @ > 90 %
Impossibile creare il servizio di bilanciamento del carico	Creazione del servizio di bilanciamento del carico non riuscita		Critico
Mancata corrispondenza della replica del carico di lavoro	Alcuni pod non sono attualmente disponibili per un Deployment o un DaemonSet.		Attenzione @ > 1
Richieste CPU ResourceQuota in procinto di superare	Le richieste di CPU per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %

Alta velocità di ritrasmissione	Elevata velocità di ritrasmissione TCP	Verifica la congestione della rete: identifica i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware.	Attenzione @ > 10 % Critico @ > 25 %
Pressione del disco del nodo	Lo spazio su disco disponibile e gli inode sul file system radice o sul file system immagine del nodo hanno soddisfatto una soglia di espulsione.	- Aumentare le dimensioni dei dischi dei nodi per garantire che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre l'utilizzo dei file dell'applicazione.	Critico @ > 0
Saturazione CPU cluster elevata	La saturazione della CPU allocabile nel cluster è elevata. La saturazione della CPU del cluster viene calcolata come la somma dell'utilizzo della CPU divisa per la somma delle CPU allocabili su tutti i nodi K8.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare CPU sui nodi.	Attenzione @ > 80 % Critico @ > 90 %

Torna all'inizio

Monitor del registro delle modifiche

Nome del monitor	Gravità	Descrizione del monitor
Volume interno scoperto	Informativo	Questo messaggio viene visualizzato quando viene rilevato un volume interno.
Volume interno modificato	Informativo	Questo messaggio viene visualizzato quando viene modificato un volume interno.
Nodo di archiviazione scoperto	Informativo	Questo messaggio viene visualizzato quando viene rilevato un nodo di archiviazione.
Nodo di archiviazione rimosso	Informativo	Questo messaggio viene visualizzato quando viene rimosso un nodo di archiviazione.
Pool di archiviazione scoperto	Informativo	Questo messaggio viene visualizzato quando viene rilevato un pool di archiviazione.

Macchina virtuale di archiviazione scoperta	Informativo	Questo messaggio viene visualizzato quando viene rilevata una macchina virtuale di archiviazione.
Macchina virtuale di archiviazione modificata	Informativo	Questo messaggio viene visualizzato quando viene modificata una macchina virtuale di archiviazione.

Torna all'inizio

Monitor di raccolta dati

Nome del monitor	Descrizione	Azione correttiva
Arresto dell'unità di acquisizione	Le unità di acquisizione Data Infrastructure Insights vengono riavviate periodicamente come parte degli aggiornamenti per introdurre nuove funzionalità. In un ambiente tipico, questo accade una volta al mese o meno. Un avviso di avviso che segnala l'arresto di un'unità di acquisizione dovrebbe essere seguito subito dopo da una risoluzione che segnala che l'unità di acquisizione appena riavviata ha completato una registrazione con Data Infrastructure Insights. In genere, il ciclo di spegnimento-registrazione dura dai 5 ai 15 minuti.	Se l'avviso si verifica frequentemente o dura più di 15 minuti, verificare il funzionamento del sistema che ospita l'Unità di acquisizione, della rete e di qualsiasi proxy che collega l'AU a Internet.
Collettore fallito	Il sondaggio di un raccoglitore di dati ha riscontrato una situazione di errore imprevista.	Per saperne di più sulla situazione, visita la pagina del raccoglitore dati in Data Infrastructure Insights .
Avviso al collezionista	Questo avviso può in genere verificarsi a causa di una configurazione errata del raccoglitore dati o del sistema di destinazione. Rivedere le configurazioni per evitare futuri avvisi. Può anche essere dovuto al recupero di dati incompleti, mentre il raccoglitore di dati ha raccolto tutti i dati che poteva. Ciò può accadere quando le situazioni cambiano durante la raccolta dei dati (ad esempio, una macchina virtuale presente all'inizio della raccolta dei dati viene eliminata durante la raccolta dei dati e prima che i dati vengano acquisiti).	Controllare la configurazione del raccoglitore dati o del sistema di destinazione. Si noti che il monitor per Collector Warning può inviare più avvisi rispetto ad altri tipi di monitor, pertanto si consiglia di non impostare alcun destinatario di avviso, a meno che non si stia risolvendo un problema.

Torna all'inizio

Monitor di sicurezza

Nome del monitor	Soglia	Descrizione del monitor	Azione correttiva
AutoSupport HTTPS AutoSupport disabilitato	Attenzione @ < 1	AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. Data la natura sensibile dei messaggi AutoSupport , NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio dei messaggi AutoSupport al supporto NetApp .	Per impostare HTTPS come protocollo di trasporto per i messaggi AutoSupport , eseguire il seguente comando ONTAP :…system node autosupport modify -transport https
Cifrari non sicuri del cluster per SSH	Attenzione @ < 1	Indica che SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	Per rimuovere i cifrari CBC, eseguire il seguente comando ONTAP :…security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Banner di accesso al cluster disabilitato	Attenzione @ < 1	Indica che il banner di accesso è disabilitato per gli utenti che accedono al sistema ONTAP . La visualizzazione di un banner di accesso è utile per stabilire le aspettative relative all'accesso e all'utilizzo del sistema.	Per configurare il banner di accesso per un cluster, eseguire il seguente comando ONTAP :…security login banner modify -vserver <admin svm> -message "Accesso limitato agli utenti autorizzati"

Comunicazione peer del cluster non crittografata	Attenzione @ < 1	Quando si replicano dati per il ripristino di emergenza, la memorizzazione nella cache o il backup, è necessario proteggere tali dati durante il trasporto via cavo da un cluster ONTAP a un altro. La crittografia deve essere configurata sia sul cluster di origine che su quello di destinazione.	Per abilitare la crittografia sulle relazioni tra peer del cluster create prima di ONTAP 9.6, il cluster di origine e quello di destinazione devono essere aggiornati alla versione 9.6. Quindi utilizzare il comando "cluster peer modify" per modificare sia i peer del cluster di origine che quelli di destinazione in modo che utilizzino la crittografia del peering del cluster. Per i dettagli, consultare la Guida al rafforzamento della sicurezza NetApp per ONTAP 9.
Utente amministratore locale predefinito abilitato	Attenzione @ > 0	NetApp consiglia di bloccare (disabilitare) tutti gli account utente amministratore predefiniti (integrati) non necessari con il comando lock. Si tratta principalmente di account predefiniti le cui password non sono mai state aggiornate o modificate.	Per bloccare l'account "admin" predefinito, eseguire il seguente comando ONTAP :…security login lock -username admin
Modalità FIPS disabilitata	Attenzione @ < 1	Quando è abilitata la conformità FIPS 140-2, TLSv1 e SSLv3 sono disabilitati e rimangono abilitati solo TLSv1.1 e TLSv1.2. ONTAP impedisce di abilitare TLSv1 e SSLv3 quando è abilitata la conformità FIPS 140-2.	Per abilitare la conformità FIPS 140-2 su un cluster, eseguire il seguente comando ONTAP in modalità privilegio avanzata:…security config modify -interface SSL -is -fips-enabled true

Inoltro del registro non crittografato	Attenzione @ < 1	Lo scaricamento delle informazioni syslog è necessario per limitare la portata o l'impatto di una violazione su un singolo sistema o soluzione. Pertanto, NetApp consiglia di scaricare in modo sicuro le informazioni syslog in un luogo di archiviazione o conservazione sicuro.	Una volta creata una destinazione di inoltro dei log, il suo protocollo non può essere modificato. Per passare a un protocollo crittografato, eliminare e ricreare la destinazione di inoltro del registro utilizzando il seguente comando ONTAP :…cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted
Password con hash MD5	Attenzione @ > 0	NetApp consiglia vivamente di utilizzare la funzione hash SHA-512 più sicura per le password degli account utente ONTAP . Gli account che utilizzano la funzione hash MD5 meno sicura dovrebbero migrare alla funzione hash SHA-512.	NetApp consiglia vivamente agli account utente di migrare alla soluzione SHA-512 più sicura, chiedendo agli utenti di modificare le proprie password. Per bloccare gli account con password che utilizzano la funzione hash MD5, eseguire il seguente comando ONTAP : security login lock -vserver * -username * -hash -function md5
Nessun server NTP è configurato	Attenzione @ < 1	Indica che il cluster non ha server NTP configurati. Per garantire ridondanza e un servizio ottimale, NetApp consiglia di associare almeno tre server NTP al cluster.	Per associare un server NTP al cluster, eseguire il seguente comando ONTAP : cluster time-service ntp server create -server <nome host o indirizzo IP del server ntp>
Il numero di server NTP è basso	Attenzione @ < 3	Indica che il cluster ha meno di 3 server NTP configurati. Per garantire ridondanza e un servizio ottimale, NetApp consiglia di associare almeno tre server NTP al cluster.	Per associare un server NTP al cluster, eseguire il seguente comando ONTAP :…cluster time-service ntp server create -server <nome host o indirizzo IP del server ntp>

Shell remota abilitata	Attenzione @ > 0	Remote Shell non è un metodo sicuro per stabilire l'accesso tramite riga di comando alla soluzione ONTAP . Per un accesso remoto sicuro, Remote Shell deve essere disabilitato.	NetApp consiglia Secure Shell (SSH) per l'accesso remoto sicuro. Per disabilitare la shell remota su un cluster, eseguire il seguente comando ONTAP in modalità privilegio avanzato: security protocol modify -application rsh- enabled false
Registro di controllo della VM di archiviazione disabilitato	Attenzione @ < 1	Indica che la registrazione di controllo è disabilitata per SVM.	Per configurare il registro di controllo per un vserver, eseguire il seguente comando ONTAP :…vserver audit enable -vserver <svm>
Cifrature non sicure per SSH nella VM di archiviazione	Attenzione @ < 1	Indica che SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	Per rimuovere i cifrari CBC, eseguire il seguente comando ONTAP :…security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Banner di accesso alla VM di archiviazione disabilitato	Attenzione @ < 1	Indica che il banner di accesso è disabilitato per gli utenti che accedono alle SVM sul sistema. La visualizzazione di un banner di accesso è utile per stabilire le aspettative relative all'accesso e all'utilizzo del sistema.	Per configurare il banner di accesso per un cluster, eseguire il seguente comando ONTAP :…security login banner modify -vserver <svm> -message "Accesso limitato agli utenti autorizzati"
Protocollo Telnet abilitato	Attenzione @ > 0	Telnet non è un metodo sicuro per stabilire l'accesso tramite riga di comando alla soluzione ONTAP . Per un accesso remoto sicuro, Telnet dovrebbe essere disabilitato.	NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro. Per disabilitare Telnet su un cluster, eseguire il seguente comando ONTAP in modalità privilegio avanzato:…security protocol modify -application telnet -enabled false

Torna all'inizio

Monitor della protezione dei dati

Nome del monitor	Soglie	Descrizione del monitor	Azione correttiva
Spazio insufficiente per la copia snapshot LUN	(Filtro contains_luns = Sì) Avviso @ > 95 %…Critico @ > 100 %	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Una parte di questo spazio, denominato spazio riservato agli snapshot, viene utilizzata per archiviare gli snapshot che consentono di proteggere i dati a livello locale. Maggiore è la quantità di dati nuovi e aggiornati memorizzati nel volume ONTAP , maggiore è la capacità di snapshot utilizzata e minore sarà la capacità di archiviazione snapshot disponibile per futuri dati nuovi o aggiornati. Se la capacità dei dati snapshot all'interno di un volume raggiunge lo spazio di riserva totale degli snapshot, il cliente potrebbe non essere in grado di archiviare nuovi dati snapshot e potrebbe verificarsi una riduzione del livello di protezione dei dati nelle LUN del volume. Il monitoraggio della capacità snapshot del volume utilizzato garantisce la continuità dei servizi dati.	**Azioni immediate** Se viene superata la soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena. 2. Elimina alcuni vecchi snapshot indesiderati per liberare spazio. **Azioni da intraprendere a breve** Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti azioni: 1. Aumentare lo spazio di riserva degli snapshot all'interno del volume per adattarsi alla crescita. 2. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena.

Ritardo nella relazione SnapMirror	Attenzione @ > 150%…Critico @ > 300%	Il ritardo nella relazione SnapMirror è la differenza tra il timestamp dello snapshot e l'ora sul sistema di destinazione. lag_time_percent è il rapporto tra il tempo di ritardo e l'intervallo di pianificazione della policy SnapMirror . Se il tempo di ritardo è uguale all'intervallo di pianificazione, lag_time_percent sarà pari al 100%. Se il criterio SnapMirror non ha una pianificazione, lag_time_percent non verrà calcolato.	Monitorare lo stato SnapMirror utilizzando il comando "snapmirror show". Controlla la cronologia dei trasferimenti SnapMirror usando il comando "snapmirror show-history"

Torna all'inizio

Monitor del volume delle nuvole (CVO)

Nome del monitor	Gravità CI	Descrizione del monitor	Azione correttiva
Disco CVO fuori servizio	INFORMAZIONI	Questo evento si verifica quando un disco viene rimosso dal servizio perché è stato contrassegnato come guasto, è in fase di sanificazione o è entrato nel Centro di manutenzione.	Nessuno

Restituzione CVO del pool di archiviazione non riuscita	CRITICO	Questo evento si verifica durante la migrazione di un aggregato come parte di un giveback di failover di archiviazione (SFO), quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive: verificare che il LIF intercluster sia online e funzionante utilizzando il comando "network interface show". Verificare la connettività di rete al server di archiviazione degli oggetti utilizzando il comando "ping" sul nodo di destinazione intercluster LIF. Verificare che la configurazione dell'archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette utilizzando il comando "aggregate object-store config show". In alternativa, è possibile ignorare l'errore specificando false per il parametro "require-partner-waiting" del comando giveback. Per ulteriori informazioni o assistenza, contattare l'assistenza tecnica NetApp .

Interconnessione CVO HA inattiva	AVVERTIMENTO	L'interconnessione ad alta disponibilità (HA) non funziona. Rischio di interruzione del servizio quando il failover non è disponibile.	Le azioni correttive dipendono dal numero e dal tipo di collegamenti di interconnessione HA supportati dalla piattaforma, nonché dal motivo per cui l'interconnessione non funziona. Se i collegamenti non funzionano: verificare che entrambi i controller nella coppia HA siano operativi. Per i collegamenti collegati esternamente, assicurarsi che i cavi di interconnessione siano collegati correttamente e che i moduli SFP (Small Form-Factor Pluggable), se applicabili, siano posizionati correttamente su entrambi i controller. Per i collegamenti collegati internamente, disattivare e riattivare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link off" e "ic link on". Se i collegamenti sono disabilitati, abilitarli utilizzando il comando "ic link on". Se un peer non è connesso, disattivare e riattivare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link off" e "ic link on". Se il problema persiste, contattare l'assistenza tecnica NetApp .

Superato il numero massimo di sessioni CVO per utente	AVVERTIMENTO	Hai superato il numero massimo di sessioni consentite per utente su una connessione TCP. Ogni richiesta di stabilire una sessione verrà respinta finché alcune sessioni non saranno rilasciate.	Eseguire le seguenti azioni correttive: ispezionare tutte le applicazioni in esecuzione sul client e terminare quelle che non funzionano correttamente. Riavviare il client. Verificare se il problema è causato da un'applicazione nuova o esistente: se l'applicazione è nuova, impostare una soglia più alta per il client utilizzando il comando "cifs option modify -max-opens-same -file-per-tree". In alcuni casi i clienti funzionano come previsto, ma richiedono una soglia più alta. Dovresti avere privilegi avanzati per impostare una soglia più alta per il client. Se il problema è causato da un'applicazione esistente, potrebbe esserci un problema con il client. Per ulteriori informazioni o assistenza, contattare l'assistenza tecnica NetApp .

Conflitto di nomi NetBIOS CVO	CRITICO	Il servizio nomi NetBIOS ha ricevuto una risposta negativa a una richiesta di registrazione del nome da un computer remoto. In genere ciò è causato da un conflitto nel nome NetBIOS o in un alias. Di conseguenza, i client potrebbero non essere in grado di accedere ai dati o di connettersi al nodo di distribuzione dei dati corretto nel cluster.	Eseguire una delle seguenti azioni correttive: Se si verifica un conflitto nel nome NetBIOS o in un alias, eseguire una delle seguenti operazioni: Eliminare l'alias NetBIOS duplicato utilizzando il comando "vserver cifs delete -aliases alias -vserver vserver". Rinominare un alias NetBIOS eliminando il nome duplicato e aggiungendo un alias con un nuovo nome utilizzando il comando "vserver cifs create -aliases alias -vserver vserver". Se non sono configurati alias e si verifica un conflitto nel nome NetBIOS, rinominare il server CIFS utilizzando i comandi "vserver cifs delete -vserver vserver" e "vserver cifs create -cifs -server netbiosname". NOTA: l'eliminazione di un server CIFS può rendere i dati inaccessibili. Rimuovere il nome NetBIOS o rinominare il NetBIOS sul computer remoto.
Pool di archiviazione CVO NFSv4 esaurito	CRITICO	Un pool di archiviazione NFSv4 è esaurito.	Se il server NFS non risponde per più di 10 minuti dopo questo evento, contattare l'assistenza tecnica NetApp .
Panico del nodo CVO	AVVERTIMENTO	Questo evento viene emesso quando si verifica un panico	Contattare l'assistenza clienti NetApp .

Spazio basso nel volume radice del nodo CVO	CRITICO	Il sistema ha rilevato che lo spazio disponibile nel volume root è pericolosamente basso. Il nodo non è completamente operativo. È possibile che i LIF dei dati siano falliti all'interno del cluster, per cui l'accesso NFS e CIFS è limitato sul nodo. La capacità amministrativa è limitata alle procedure di ripristino locale del nodo per liberare spazio sul volume radice.	Eseguire le seguenti azioni correttive: liberare spazio sul volume root eliminando le vecchie copie Snapshot, eliminando i file non più necessari dalla directory /mroot o espandendo la capacità del volume root. Riavviare il controller. Per ulteriori informazioni o assistenza, contattare l'assistenza tecnica NetApp .
Condivisione amministratore inesistente CVO	CRITICO	Problema Vscan: un client ha tentato di connettersi a una condivisione ONTAP_ADMIN$ inesistente.	Assicurarsi che Vscan sia abilitato per l'ID SVM menzionato. L'abilitazione di Vscan su una SVM determina la creazione automatica della condivisione ONTAP_ADMIN$ per la SVM.
Host archivio oggetti CVO non risolvibile	CRITICO	Il nome host del server di archiviazione degli oggetti non può essere risolto in un indirizzo IP. Il client dell'archivio oggetti non può comunicare con il server dell'archivio oggetti senza risolvere un indirizzo IP. Di conseguenza, i dati potrebbero risultare inaccessibili.	Controllare la configurazione DNS per verificare che il nome host sia configurato correttamente con un indirizzo IP.
CVO Object Store Intercluster LIF inattivo	CRITICO	Il client dell'archivio oggetti non riesce a trovare un LIF operativo per comunicare con il server dell'archivio oggetti. Il nodo non consentirà il traffico client dell'archivio oggetti finché il LIF intercluster non sarà operativo. Di conseguenza, i dati potrebbero risultare inaccessibili.	Eseguire le seguenti azioni correttive: verificare lo stato LIF intercluster utilizzando il comando "network interface show -role intercluster". Verificare che il LIF intercluster sia configurato correttamente e operativo. Se non è configurato un LIF intercluster, aggiungerlo utilizzando il comando "network interface create -role intercluster".

Mancata corrispondenza della firma dell'archivio oggetti CVO	CRITICO	La firma della richiesta inviata al server dell'archivio oggetti non corrisponde alla firma calcolata dal client. Di conseguenza, i dati potrebbero risultare inaccessibili.	Verificare che la chiave di accesso segreta sia configurata correttamente. Se la configurazione è corretta, contattare il supporto tecnico NetApp per ricevere assistenza.
Memoria monitor QoS CVO esaurita	CRITICO	La memoria dinamica del sottosistema QoS ha raggiunto il limite per l'hardware della piattaforma attuale. Alcune funzionalità QoS potrebbero funzionare con capacità limitata.	Eliminare alcuni carichi di lavoro o flussi attivi per liberare memoria. Utilizzare il comando "statistics show -object workload -counter ops" per determinare quali carichi di lavoro sono attivi. I carichi di lavoro attivi mostrano operazioni diverse da zero. Quindi utilizzare più volte il comando "workload delete <workload_name>" per rimuovere carichi di lavoro specifici. In alternativa, utilizzare il comando "stream delete -workload <nome carico di lavoro> *" per eliminare i flussi associati dal carico di lavoro attivo.

Timeout CVO READDIR	CRITICO	Un’operazione sul file READDIR ha superato il timeout consentito per l’esecuzione in WAFL. Ciò può essere dovuto a directory molto grandi o sparse. Si raccomanda un’azione correttiva.	Eseguire le seguenti azioni correttive: trovare informazioni specifiche sulle directory recenti le cui operazioni sui file READDIR sono scadute utilizzando il seguente comando CLI nodeshell con privilegio 'diag': wafl readdir notice show. Controllare se le directory sono indicate come sparse o meno: se una directory è indicata come sparse, si consiglia di copiare il contenuto della directory in una nuova directory per rimuovere la scarsità del file della directory. Se una directory non è indicata come sparse e la directory è di grandi dimensioni, si consiglia di ridurre le dimensioni del file della directory riducendo il numero di voci di file nella directory.

Errore di rilocazione CVO del pool di archiviazione	CRITICO	Questo evento si verifica durante lo spostamento di un aggregato, quando il nodo di destinazione non riesce a raggiungere gli archivi degli oggetti.	Eseguire le seguenti azioni correttive: verificare che il LIF intercluster sia online e funzionante utilizzando il comando "network interface show". Verificare la connettività di rete al server di archiviazione degli oggetti utilizzando il comando "ping" sul nodo di destinazione intercluster LIF. Verificare che la configurazione dell'archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette utilizzando il comando "aggregate object-store config show". In alternativa, è possibile ignorare l'errore utilizzando il parametro "override-destination-checks" del comando di rilocazione. Per ulteriori informazioni o assistenza, contattare l'assistenza tecnica NetApp .
Copia shadow CVO non riuscita	CRITICO	Si è verificato un errore nel servizio Copia Shadow del volume (VSS), un'operazione di backup e ripristino del servizio Microsoft Server.	Verificare quanto segue utilizzando le informazioni fornite nel messaggio dell'evento: la configurazione della copia shadow è abilitata? Sono installate le licenze appropriate? Su quali condivisioni viene eseguita l'operazione di copia shadow? Il nome della condivisione è corretto? Esiste il percorso di condivisione? Quali sono gli stati del set di copie shadow e delle sue copie shadow?
Arresto riuscito della VM di archiviazione CVO	INFORMAZIONI	Questo messaggio viene visualizzato quando un'operazione di 'arresto del vserver' riesce.	Utilizzare il comando 'vserver start' per avviare l'accesso ai dati su una VM di archiviazione.

CVO Troppe autenticazioni CIFS	AVVERTIMENTO	Si sono verificate contemporaneamente numerose negoziazioni di autenticazione. Ci sono 256 richieste di nuove sessioni incomplete da questo client.	Indagare sul motivo per cui il client ha creato 256 o più nuove richieste di connessione. Potrebbe essere necessario contattare il fornitore del client o dell'applicazione per determinare il motivo per cui si è verificato l'errore.
Dischi CVO non assegnati	INFORMAZIONI	Il sistema ha dischi non assegnati: la capacità viene sprecata e potrebbe essere stata applicata una configurazione errata o una modifica parziale della configurazione del sistema.	Eseguire le seguenti azioni correttive: determinare quali dischi non sono assegnati utilizzando il comando "disk show -n". Assegnare i dischi a un sistema utilizzando il comando "disk assign".
Accesso utente non autorizzato CVO alla condivisione amministrativa	AVVERTIMENTO	Un client ha tentato di connettersi alla condivisione privilegiata ONTAP_ADMIN$ anche se l'utente connesso non è un utente autorizzato.	Eseguire le seguenti azioni correttive: assicurarsi che il nome utente e l'indirizzo IP menzionati siano configurati in uno dei pool di scanner Vscan attivi. Controllare la configurazione del pool di scanner attualmente attivo utilizzando il comando "vserver vscan scanner pool show-active".
Rilevato virus CVO	AVVERTIMENTO	Un server Vscan ha segnalato un errore al sistema di archiviazione. In genere questo indica che è stato trovato un virus. Tuttavia, altri errori sul server Vscan possono causare questo evento. L'accesso del client al file è negato. A seconda delle impostazioni e della configurazione, il server Vscan potrebbe pulire il file, metterlo in quarantena o eliminarlo.	Controllare il registro del server Vscan riportato nell'evento "syslog" per verificare se è riuscito a pulire, mettere in quarantena o eliminare correttamente il file infetto. Se ciò non fosse possibile, un amministratore di sistema potrebbe dover eliminare manualmente il file.
Volume CVO offline	INFORMAZIONI	Questo messaggio indica che un volume è stato reso offline.	Ripristinare il volume online.

Volume CVO limitato	INFORMAZIONI	Questo evento indica che un volume flessibile è stato reso limitato.	Ripristinare il volume online.

Torna all'inizio

Monitoraggio dei log dei mediatori SnapMirror for Business Continuity (SMBC)

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Aggiunto mediatore ONTAP	INFORMAZIONI	Questo messaggio viene visualizzato quando ONTAP Mediator viene aggiunto correttamente a un cluster.	Nessuno
Mediatore ONTAP non accessibile	CRITICO	Questo messaggio viene visualizzato quando ONTAP Mediator viene riadattato oppure il pacchetto Mediator non è più installato sul server Mediator. Di conseguenza, il failover SnapMirror non è possibile.	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Rimosso il mediatore ONTAP	INFORMAZIONI	Questo messaggio viene visualizzato quando ONTAP Mediator viene rimosso correttamente da un cluster.	Nessuno
Mediatore ONTAP irraggiungibile	AVVERTIMENTO	Questo messaggio viene visualizzato quando il mediatore ONTAP non è raggiungibile su un cluster. Di conseguenza, il failover SnapMirror non è possibile.	Verificare la connettività di rete al mediatore ONTAP utilizzando i comandi "network ping" e "network traceroute". Se il problema persiste, rimuovere la configurazione dell'attuale ONTAP Mediator utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".

Certificato CA SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato dell'autorità di certificazione (CA) ONTAP Mediator è scaduto. Di conseguenza, non sarà possibile alcuna ulteriore comunicazione con il mediatore ONTAP .	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato CA sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato CA SMBC in scadenza	AVVERTIMENTO	Questo messaggio viene visualizzato quando il certificato dell'autorità di certificazione (CA) ONTAP Mediator scade entro i prossimi 30 giorni.	Prima che questo certificato scada, rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato CA sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato client SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato client ONTAP Mediator è scaduto. Di conseguenza, non sarà possibile alcuna ulteriore comunicazione con il mediatore ONTAP .	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato client SMBC in scadenza	AVVERTIMENTO	Questo messaggio viene visualizzato quando il certificato client ONTAP Mediator scade entro i prossimi 30 giorni.	Prima che questo certificato scada, rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".

Relazione SMBC fuori sincrono Nota: UM non ha questo	CRITICO	Questo messaggio viene visualizzato quando una relazione SnapMirror for Business Continuity (SMBC) cambia stato da "in sincronia" a "non sincronizzata". A causa di questo RPO=0 la protezione dei dati verrà interrotta.	Controllare la connessione di rete tra i volumi di origine e di destinazione. Monitorare lo stato della relazione SMBC utilizzando il comando "snapmirror show" sulla destinazione e il comando "snapmirror list-destinations" sulla sorgente. La risincronizzazione automatica tenterà di riportare la relazione allo stato "sincronizzata". Se la risincronizzazione fallisce, verificare che tutti i nodi del cluster siano in quorum e integri.
Certificato del server SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato del server ONTAP Mediator è scaduto. Di conseguenza, non sarà possibile alcuna ulteriore comunicazione con il mediatore ONTAP .	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato server sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato del server SMBC in scadenza	AVVERTIMENTO	Questo messaggio viene visualizzato quando il certificato del server ONTAP Mediator scade entro i prossimi 30 giorni.	Prima che questo certificato scada, rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato server sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".

Torna all'inizio

Monitor di sistema aggiuntivi per alimentazione, battito cardiaco e altri parametri

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Scoperto l'alimentatore del ripiano del disco	INFORMATIVO	Questo messaggio viene visualizzato quando un alimentatore viene aggiunto allo scaffale dei dischi.	NESSUNO
Ripiani del disco Alimentatore rimosso	INFORMATIVO	Questo messaggio viene visualizzato quando un alimentatore viene rimosso dal ripiano del disco.	NESSUNO
Commutazione automatica non pianificata di MetroCluster disabilitata	CRITICO	Questo messaggio viene visualizzato quando la funzionalità di commutazione automatica non pianificata è disabilitata.	Eseguire il comando "metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true" per ciascun nodo del cluster per abilitare il passaggio automatico.
MetroCluster Storage Bridge non raggiungibile	CRITICO	Il bridge di archiviazione non è raggiungibile tramite la rete di gestione	1) Se il bridge è monitorato da SNMP, verificare che il LIF di gestione del nodo sia attivo utilizzando il comando "network interface show". Verificare che il bridge sia attivo utilizzando il comando "network ping". 2) Se il bridge è monitorato in banda, controllare il cablaggio fabric al bridge e quindi verificare che il bridge sia acceso.
Temperatura anomala del ponte MetroCluster - inferiore al valore critico	CRITICO	Il sensore sul bridge Fibre Channel segnala una temperatura inferiore alla soglia critica.	1) Verificare lo stato operativo delle ventole sul ponte di accumulo. 2) Verificare che il ponte funzioni alle condizioni di temperatura consigliate.

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Temperatura anomala del ponte MetroCluster - superiore al valore critico	CRITICO	Il sensore sul bridge Fibre Channel segnala una temperatura superiore alla soglia critica.	1) Verificare lo stato operativo del sensore di temperatura del telaio sullo storage bridge utilizzando il comando "storage bridge show -cooling". 2) Verificare che il ponte di archiviazione funzioni alle condizioni di temperatura consigliate.
MetroCluster Aggregate lasciato indietro	AVVERTIMENTO	L'aggregato è rimasto indietro durante il tornante.	1) Controllare lo stato dell'aggregato utilizzando il comando "aggr show". 2) Se l'aggregato è online, restituirlo al proprietario originale utilizzando il comando "metrocluster switchback".
Tutti i collegamenti tra i partner di Metrocluster sono inattivi	CRITICO	Gli adattatori di interconnessione RDMA e i LIF intercluster hanno interrotto le connessioni al cluster peered oppure il cluster peered è inattivo.	1) Assicurarsi che i LIF intercluster siano attivi e funzionanti. Riparare i LIF intercluster se sono inattivi. 2) Verificare che il cluster peer sia attivo e funzionante utilizzando il comando "cluster peer ping". Se il cluster peer è inattivo, consultare la Guida al ripristino di emergenza MetroCluster . 3) Per il fabric MetroCluster, verificare che gli ISL del fabric back-end siano attivi e funzionanti. Riparare gli ISL del fabric back-end se sono inattivi. 4) Per le configurazioni MetroCluster non fabric, verificare che il cablaggio tra gli adattatori di interconnessione RDMA sia corretto. Riconfigurare il cablaggio se i collegamenti non funzionano.

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
I partner MetroCluster non sono raggiungibili tramite la rete di peering	CRITICO	La connettività al cluster peer è interrotta.	1) Assicurarsi che la porta sia collegata alla rete/switch corretto. 2) Assicurarsi che il LIF intercluster sia connesso al cluster peer. 3) Assicurarsi che il cluster peer sia attivo e funzionante utilizzando il comando "cluster peer ping". Se il cluster peer è inattivo, fare riferimento alla Guida al ripristino di emergenza MetroCluster .
MetroCluster Inter Switch Tutti i collegamenti non attivi	CRITICO	Tutti i collegamenti Inter-Switch (ISL) sullo switch di archiviazione sono inattivi.	1) Riparare gli ISL del fabric back-end sullo switch di archiviazione. 2) Assicurarsi che lo switch del partner sia attivo e che i suoi ISL siano operativi. 3) Assicurarsi che le apparecchiature intermedie, come i dispositivi xWDM, siano operative.
Collegamento SAS tra nodo MetroCluster e stack di archiviazione non attivo	AVVERTIMENTO	Il problema potrebbe essere dovuto all'adattatore SAS o al cavo collegato.	1. Verificare che l'adattatore SAS sia online e in esecuzione. 2. Verificare che il collegamento fisico del cavo sia sicuro e funzionante e, se necessario, sostituire il cavo. 3. Se l'adattatore SAS è collegato agli scaffali dei dischi, assicurarsi che gli IOM e i dischi siano posizionati correttamente.
Collegamenti dell'iniziatore MetroClusterFC non attivi	CRITICO	L'adattatore dell'iniziatore FC è difettoso.	1. Assicurarsi che il collegamento dell'iniziatore FC non sia stato manomesso. 2. Verificare lo stato operativo dell'adattatore dell'iniziatore FC utilizzando il comando "system node run -node local -command storage show adapter".

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Collegamento di interconnessione FC-VI inattivo	CRITICO	Il collegamento fisico sulla porta FC-VI è offline.	1. Assicurarsi che il collegamento FC-VI non sia stato manomesso. 2. Verificare che lo stato fisico dell'adattatore FC-VI sia "Up" utilizzando il comando "metrocluster interconnect adapter show". 3. Se la configurazione include switch fabric, assicurarsi che siano cablati e configurati correttamente.
Dischi di riserva MetroCluster lasciati indietro	AVVERTIMENTO	Il disco di riserva è stato lasciato indietro durante il ritorno.	Se il disco non è danneggiato, restituirlo al proprietario originale utilizzando il comando "metrocluster switchback".
Porta del ponte di archiviazione MetroCluster inattiva	CRITICO	La porta sul bridge di archiviazione è offline.	1) Verificare lo stato operativo delle porte sullo storage bridge utilizzando il comando "storage bridge show -ports". 2) Verificare la connettività logica e fisica alla porta.
Ventole dello switch di archiviazione MetroCluster guaste	CRITICO	La ventola dell'interruttore di archiviazione è guasta.	1) Assicurarsi che le ventole dello switch funzionino correttamente utilizzando il comando "storage switch show -cooling". 2) Assicurarsi che le FRU delle ventole siano inserite correttamente e funzionanti.
Switch di archiviazione MetroCluster non raggiungibile	CRITICO	Lo switch di archiviazione non è raggiungibile tramite la rete di gestione.	1) Assicurarsi che il LIF di gestione del nodo sia attivo utilizzando il comando "network interface show". 2) Assicurarsi che lo switch sia attivo utilizzando il comando "network ping". 3) Assicurarsi che lo switch sia raggiungibile tramite SNMP controllando le impostazioni SNMP dopo aver effettuato l'accesso allo switch.

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Alimentatori MetroCluster Switch guasti	CRITICO	Un alimentatore sullo switch di archiviazione non è operativo.	1) Verificare i dettagli dell'errore utilizzando il comando "storage switch show -error -switch-name <nome switch>". 2) Identificare l'alimentatore difettoso utilizzando il comando "storage switch show -power -switch -name <nome switch>". 3) Assicurarsi che l'alimentatore sia correttamente inserito nel telaio dello switch di archiviazione e sia completamente funzionante.
Sensori di temperatura dell'interruttore MetroCluster guasti	CRITICO	Il sensore sullo switch Fibre Channel è guasto.	1) Verificare lo stato operativo dei sensori di temperatura sullo switch di accumulo utilizzando il comando "storage switch show -cooling". 2) Verificare che l'interruttore funzioni alle condizioni di temperatura consigliate.
Temperatura anomala dell'interruttore MetroCluster	CRITICO	Il sensore di temperatura sullo switch Fibre Channel ha segnalato una temperatura anomala.	1) Verificare lo stato operativo dei sensori di temperatura sullo switch di accumulo utilizzando il comando "storage switch show -cooling". 2) Verificare che l'interruttore funzioni alle condizioni di temperatura consigliate.
Heartbeat del processore di servizio perso	INFORMATIVO	Questo messaggio viene visualizzato quando ONTAP non riceve il segnale "heartbeat" previsto dal Service Processor (SP). Insieme a questo messaggio, verranno inviati i file di registro di SP per il debug. ONTAP reimposterà l' SP per tentare di ripristinare la comunicazione. Durante il riavvio, l' SP non sarà disponibile per un massimo di due minuti.	Contattare l'assistenza tecnica NetApp .

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Heartbeat del processore di servizio arrestato	AVVERTIMENTO	Questo messaggio viene visualizzato quando ONTAP non riceve più heartbeat dal Service Processor (SP). A seconda della progettazione hardware, il sistema potrebbe continuare a fornire dati oppure potrebbe decidere di spegnersi per evitare perdite di dati o danni all'hardware. Il sistema continua a fornire dati, ma poiché il SP potrebbe non funzionare, non è in grado di inviare notifiche di dispositivi inattivi, errori di avvio o errori POST (Power-On Self-Test) di Open Firmware (OFW). Se il sistema è configurato per farlo, genera e trasmette un messaggio AutoSupport (o "chiamata a casa") al supporto tecnico NetApp e alle destinazioni configurate. La corretta consegna di un messaggio AutoSupport migliora significativamente la determinazione e la risoluzione dei problemi.	Se il sistema si è spento, provare a eseguire un hard power cycle: estrarre il controller dallo chassis, spingerlo nuovamente dentro e accendere il sistema. Contattare l'assistenza tecnica NetApp se il problema persiste dopo il ciclo di accensione e spegnimento o per qualsiasi altra condizione che potrebbe richiedere attenzione.

Torna all'inizio

Ulteriori informazioni

- "Visualizzazione e chiusura degli avvisi"

Notifiche webhook

Notifica tramite webhook

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato.

Molte applicazioni commerciali supportano i webhook come interfaccia di input standard, ad esempio: Slack, PagerDuty, Teams e Discord supportano tutti i webhook. Grazie al supporto di un canale webhook generico e personalizzabile, Data Infrastructure Insights può supportare molti di questi canali di distribuzione. Le informazioni sui webhook sono disponibili sui siti web di queste applicazioni. Ad esempio, Slack

fornisce"questa guida utile" .

È possibile creare più canali webhook, ognuno dei quali è destinato a uno scopo diverso: applicazioni separate, destinatari diversi, ecc.

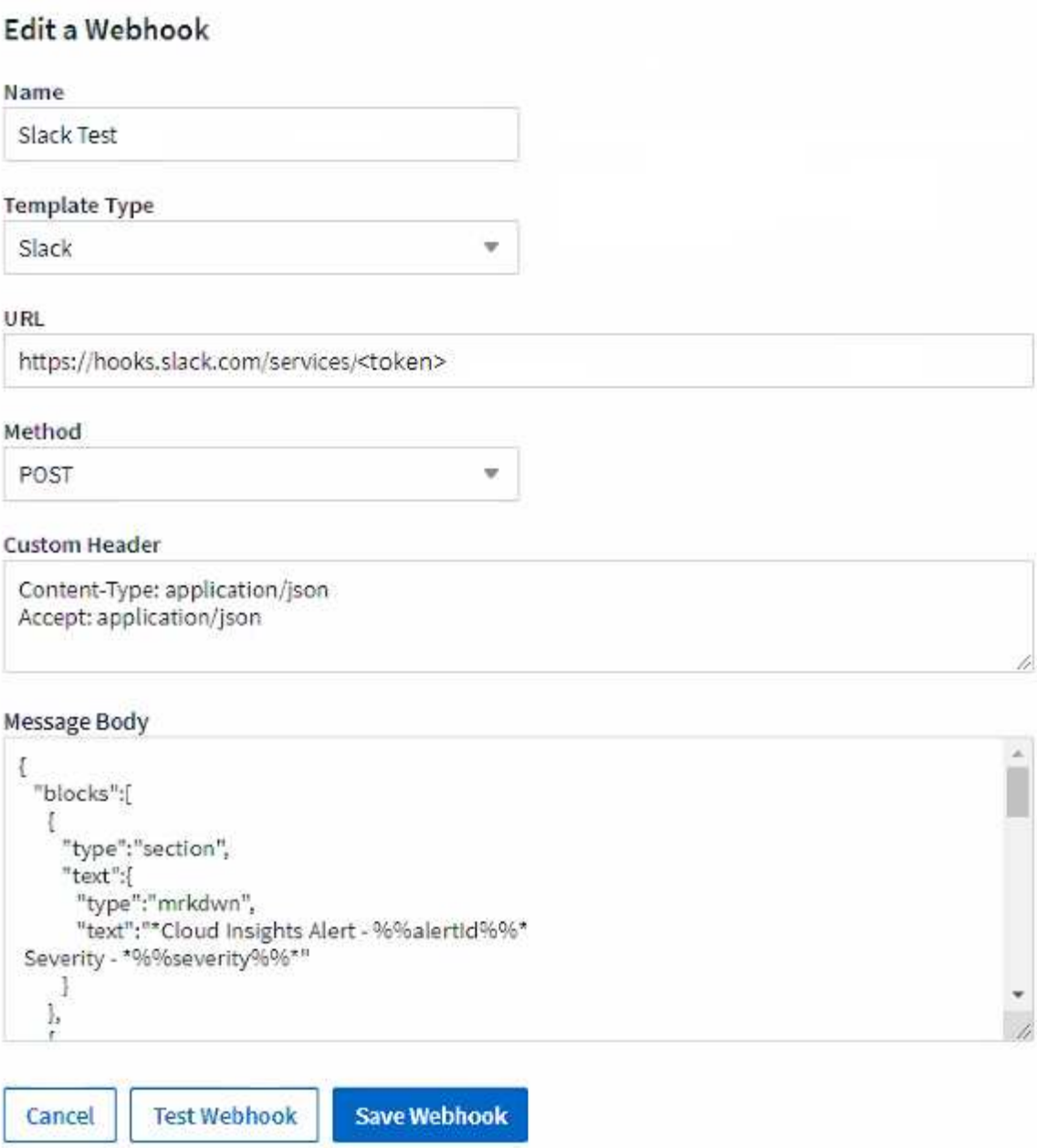
L'istanza del canale webhook è composta dai seguenti elementi:

Nome	Nome univoco
URL	URL di destinazione del webhook, incluso il prefisso *http://* o *https://* insieme ai parametri URL
Metodo	GET, POST - Il valore predefinito è POST
Intestazione personalizzata	Specifica qui eventuali righe di intestazione personalizzate
Corpo del messaggio	Inserisci qui il corpo del tuo messaggio
Parametri di avviso predefiniti	Elenca i parametri predefiniti per il webhook
Parametri e segreti personalizzati	I parametri personalizzati e i segreti consentono di aggiungere parametri univoci ed elementi sicuri come le password

Creazione di un webhook

Per creare un webhook Data Infrastructure Insights , vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**.

L'immagine seguente mostra un esempio di webhook configurato per Slack:



Inserisci le informazioni appropriate per ciascun campo e clicca su "Salva" al termine.

Puoi anche cliccare sul pulsante "Test Webhook" per testare la connessione. Si noti che in questo modo verrà inviato il "Corpo del messaggio" (senza sostituzioni) all'URL definito in base al metodo selezionato.

I webhook di Data Infrastructure Insights comprendono una serie di parametri predefiniti. Inoltre, puoi creare parametri o segreti personalizzati.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Parametri: cosa sono e come si usano?

I parametri di avviso sono valori dinamici popolati per avviso. Ad esempio, il parametro *%%TriggeredOn%%* verrà sostituito con l'oggetto su cui è stato attivato l'avviso.

È possibile aggiungere qualsiasi attributo dell'oggetto (ad esempio, il nome dell'archivio) come parametro a un webhook. Ad esempio, è possibile impostare parametri per il nome del volume e il nome dell'archiviazione in una descrizione webhook come: "Latenza elevata per volume: *%%relatedObject.volume.name%%*, Archiviazione: *%%relatedObject.storage.name%%*".

Si noti che in questa sezione le sostituzioni *non* vengono eseguite quando si fa clic sul pulsante "Test Webhook"; il pulsante invia un payload che mostra le *%%* sostituzioni ma non le sostituisce con i dati.

Parametri e segreti personalizzati

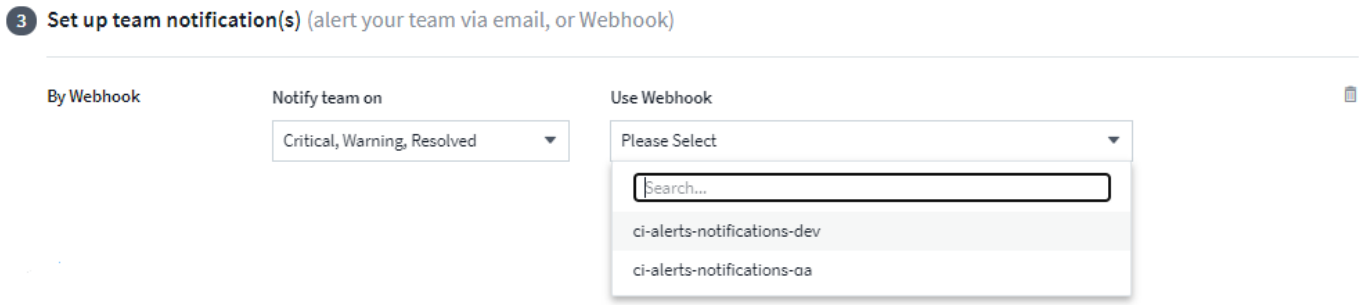
In questa sezione puoi aggiungere tutti i parametri personalizzati e/o segreti che desideri. Per motivi di sicurezza, se viene definito un segreto, solo il creatore del webhook può modificare questo canale webhook. Per gli altri è di sola lettura. È possibile utilizzare i segreti negli URL/intestazioni come *%%<secret_name>%%*.

Pagina elenco webhook

Nella pagina dell'elenco dei webhook vengono visualizzati i campi Nome, Creato da, Creato il, Stato, Sicuro e Ultimo segnalato.

Scelta della notifica webhook in un monitor

Per scegliere la notifica webhook in un"monitorare" , vai su **Avvisi > Gestisci monitor** e seleziona il monitor desiderato oppure aggiungine uno nuovo. Nella sezione *Imposta notifiche team*, seleziona *Webhook* come metodo di consegna. Selezionare i livelli di allerta (Critico, Avviso, Risolto), quindi scegliere il webhook desiderato.



Esempi di webhook:

Webhook per"Slack" Webhook per"PagerDuty" Webhook per"Squadre" Webhook per"Discordia"

Esempio di webhook per Discord

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Discord.

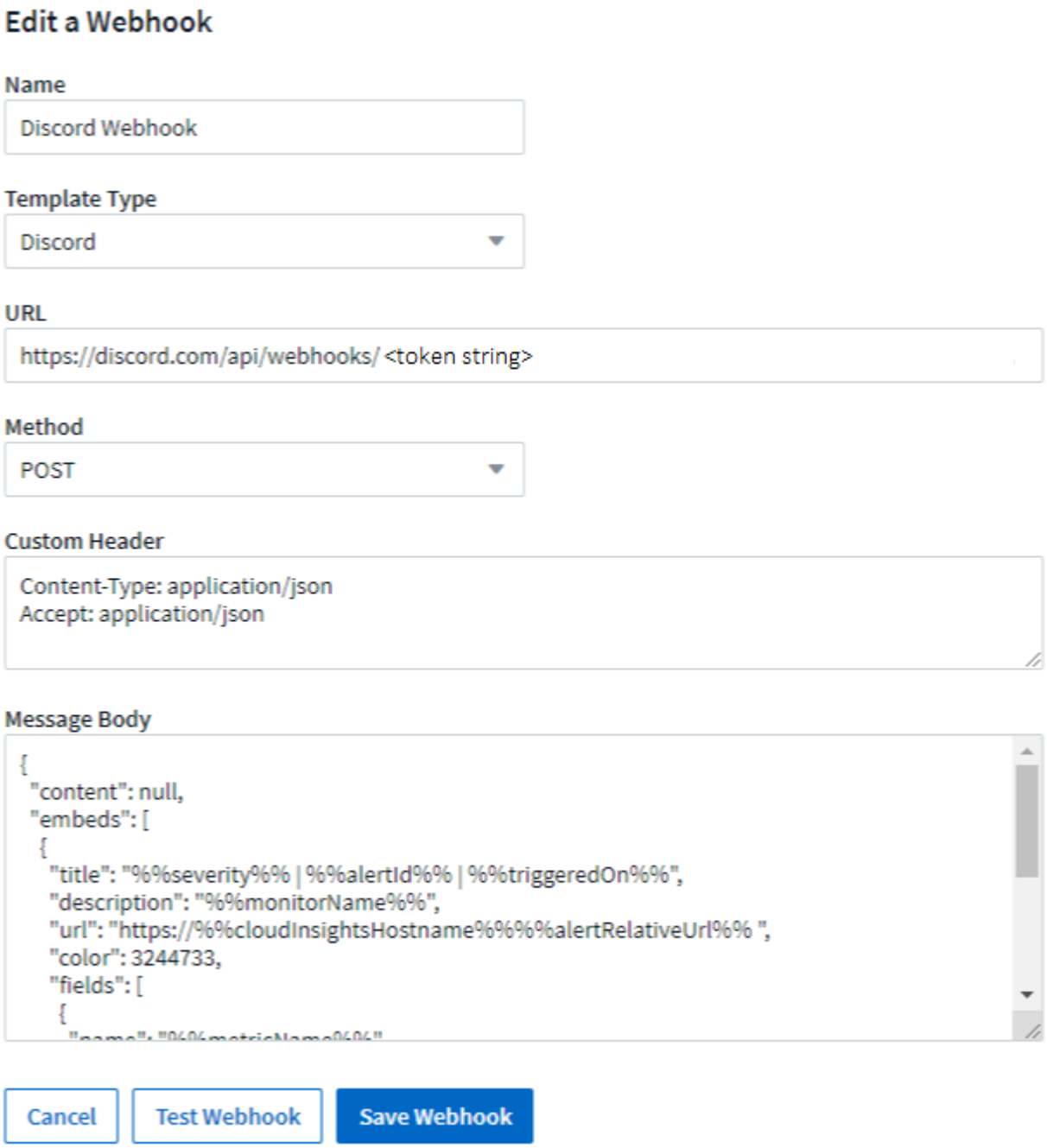
Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione Discord" per le informazioni più aggiornate.

Configurazione Discord:

- In Discord, seleziona il server, in Canali di testo, seleziona Modifica canale (icona a forma di ingranaggio)
- Seleziona **Integrazioni > Visualizza webhook** e fai clic su **Nuovo webhook**
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Data Infrastructure Insights .

Crea un webhook Data Infrastructure Insights :

1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare clic su **+Webhook** per creare un nuovo webhook.
2. Assegna al webhook un nome significativo, ad esempio "Discord".
3. Nel menu a discesa *Tipo di modello*, seleziona **Discord**.
4. Incolla l'URL sopra nel campo *URL*.

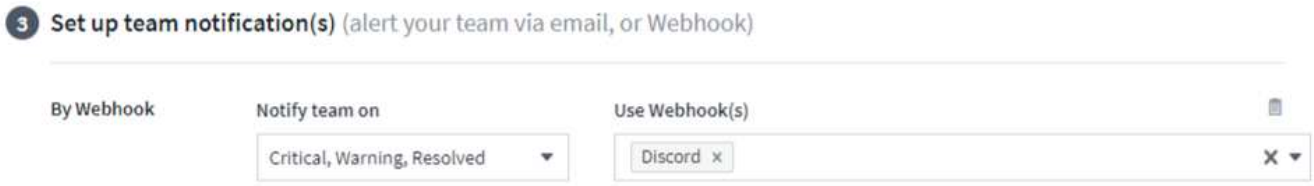


Per testare il webhook, sostituisci temporaneamente il valore URL nel corpo del messaggio con un URL valido (ad esempio *https://netapp.com*), quindi fai clic sul pulsante *Test Webhook*. Una volta completato il test, assicurati di reimpostare il corpo del messaggio.

Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.
- Seleziona il webhook "Discord" per gli eventi desiderati (Critico, Avviso, Risolto)



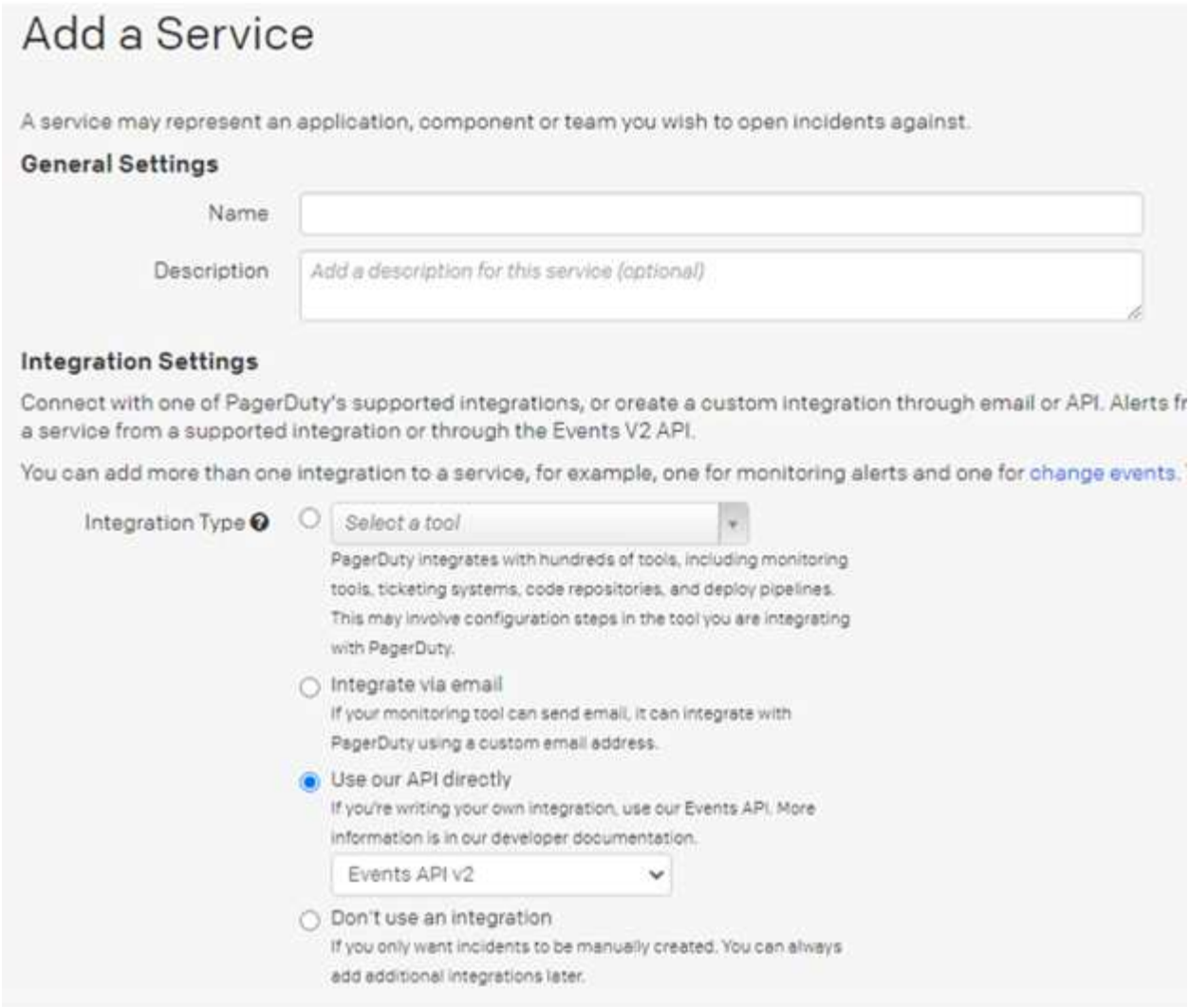
Esempio di webhook per PagerDuty

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per PagerDuty.

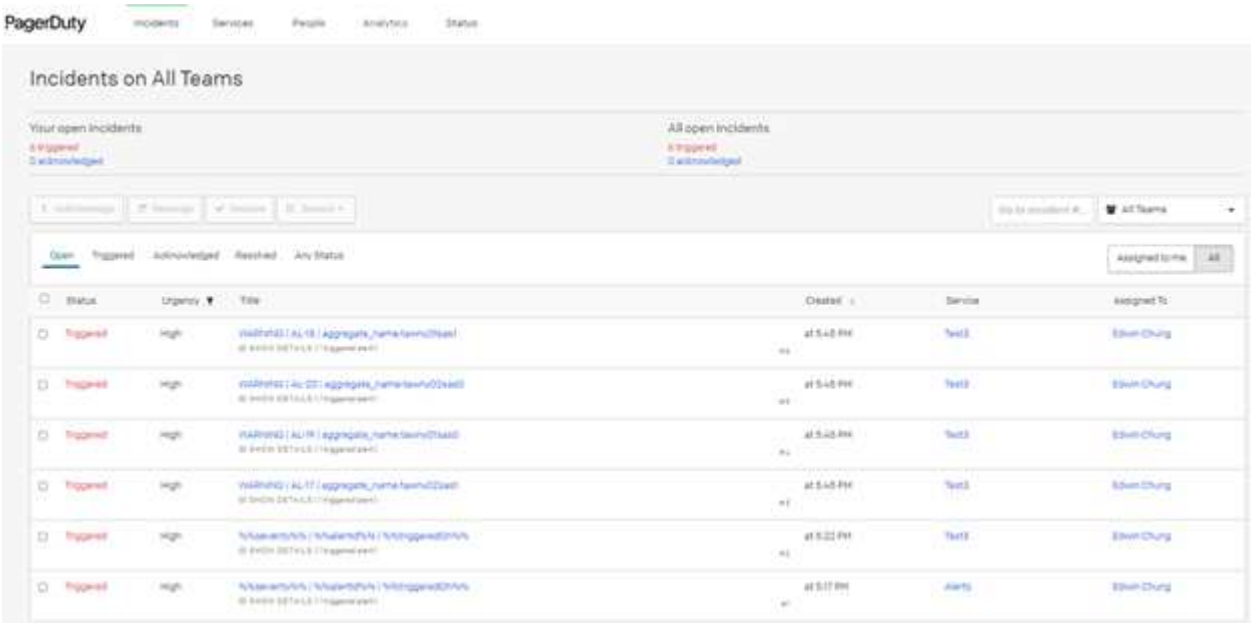
Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione PagerDuty" per le informazioni più aggiornate.

Configurazione PagerDuty:

1. In PagerDuty, vai su **Servizi > Directory dei servizi** e clicca sul pulsante **+Nuovo servizio**
2. Inserisci un *Nome* e seleziona *Usa direttamente la nostra API*. Fare clic su *Aggiungi servizio*.

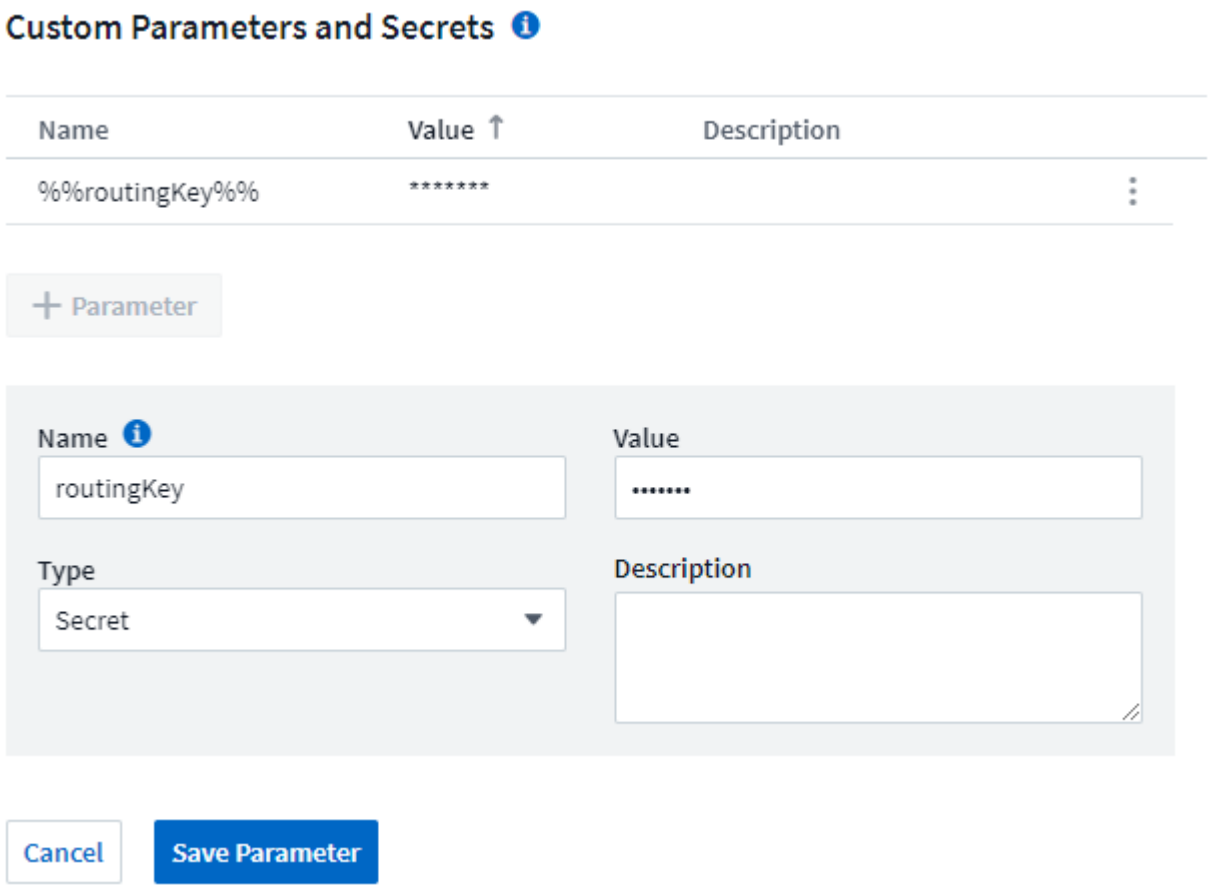


3. Fare clic sulla scheda *Integrazioni* per visualizzare la **Chiave di integrazione**. Questa chiave ti servirà quando creerai il webhook Data Infrastructure Insights riportato di seguito.
4. Vai a **Incidenti** o **Servizi** per visualizzare gli avvisi.



Crea un webhook Data Infrastructure Insights :

1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare clic su **+Webhook** per creare un nuovo webhook.
2. Assegna al webhook un nome significativo, ad esempio "PagerDuty Trigger". Utilizzerai questo webhook per eventi di livello critico e di avviso.
3. Nel menu a discesa *Tipo di modello*, seleziona **PagerDuty**.
4. Crea un parametro segreto personalizzato denominato *routingKey* e imposta il valore sul valore *Integration Key* di PagerDuty indicato sopra.



Ripetere questi passaggi per creare un webhook "PagerDuty Resolve" per gli eventi risolti.

Mappatura dei campi di PagerDuty per Data Infrastructure Insights

La tabella e l'immagine seguenti mostrano la mappatura dei campi tra PagerDuty e Data Infrastructure Insights:

PagerDuty	Data Infrastructure Insights
Tasto di avviso	ID avviso
Fonte	Attivato
Componente	Nome metrica
Gruppo	Tipo di oggetto

PagerDuty	Data Infrastructure Insights
Classe	Nome del monitor

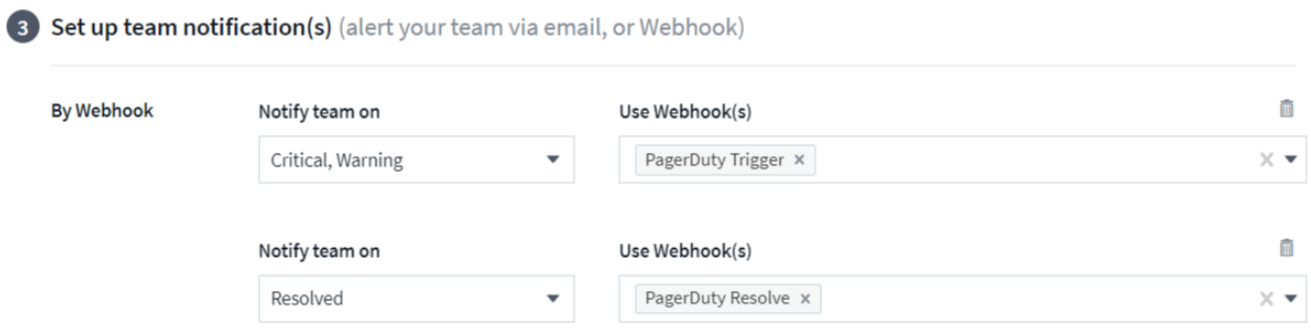
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.
- Selezionare il webhook "PagerDuty Trigger" per gli eventi di livello critico e di avviso.
- Selezionare "PagerDuty Resolve" per gli eventi risolti.



Impostare notifiche separate per gli eventi trigger rispetto agli eventi risolti è una buona pratica, poiché PagerDuty gestisce gli eventi trigger in modo diverso rispetto agli eventi risolti.

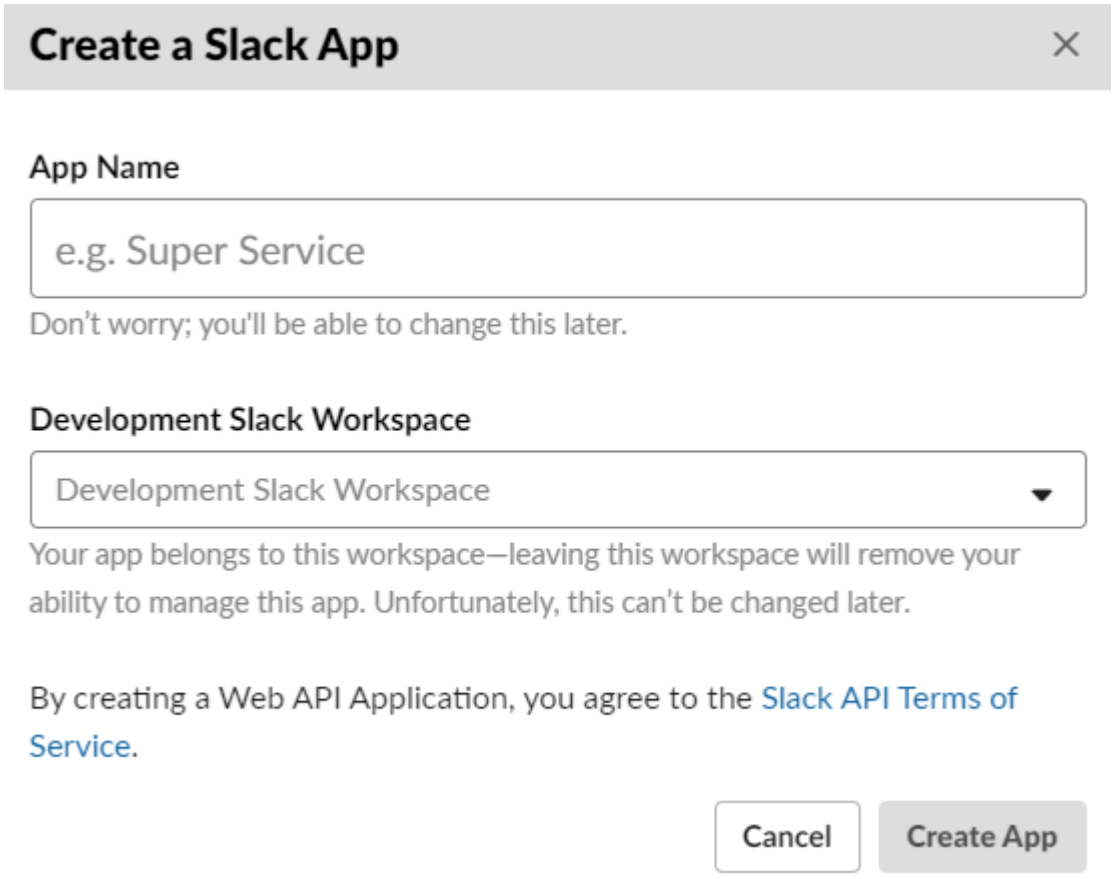
Esempio di webhook per Slack

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Slack.

Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione Slack" per le informazioni più aggiornate.

Esempio di Slack:

- Vai a https://api.slack.com/apps e crea una nuova app. Assegnagli un nome significativo e seleziona Slack Workspace.



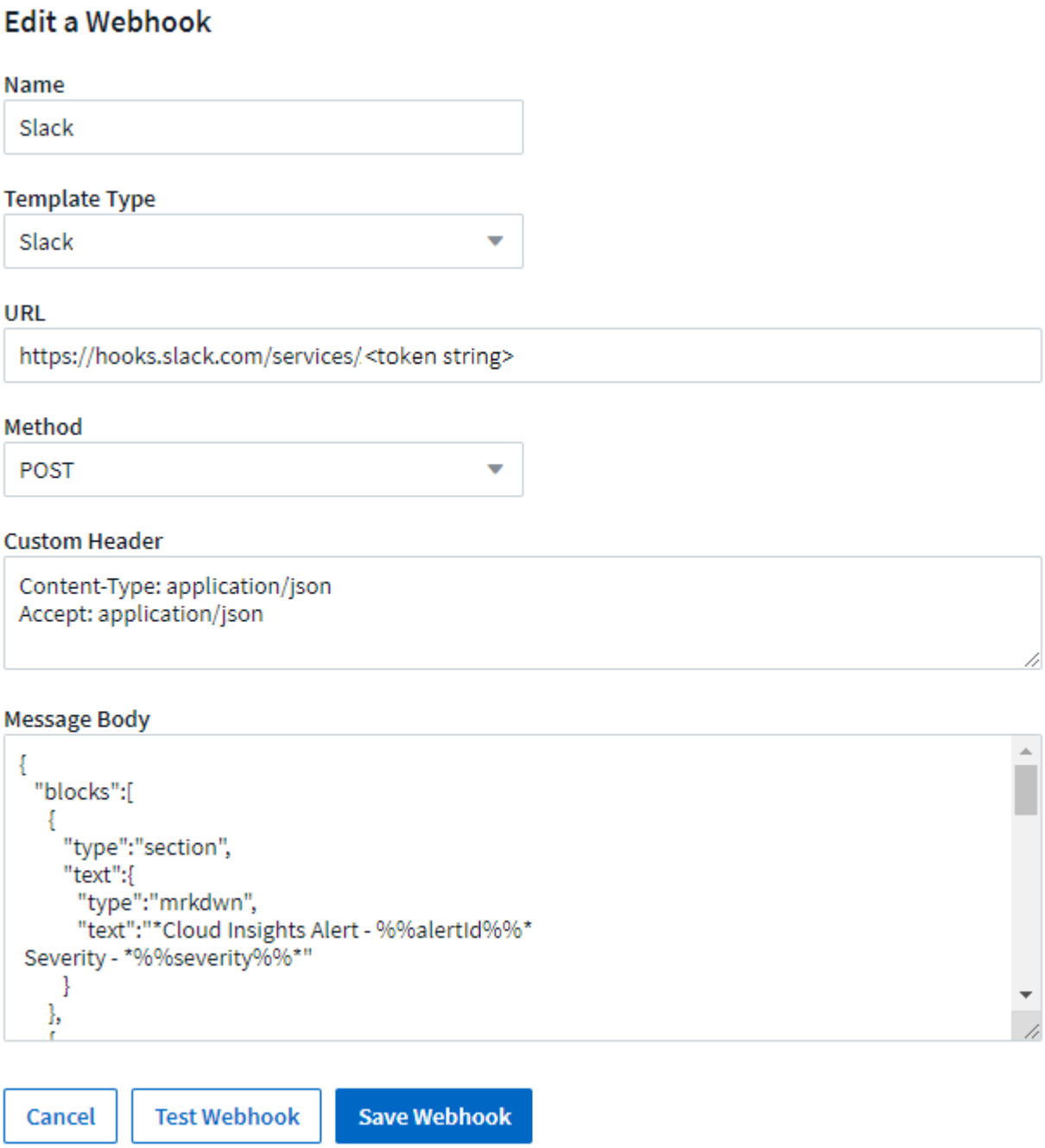
- Vai a Webhook in arrivo, clicca su *Attiva webhook in arrivo*, Richiedi di *Aggiungere nuovo webhook* e seleziona il canale su cui pubblicare.
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Data Infrastructure Insights .

Crea un webhook Data Infrastructure Insights :

1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare

clic su **+Webhook** per creare un nuovo webhook.

2. Assegna al webhook un nome significativo, ad esempio "Webhook Slack".
3. Nel menu a discesa *Tipo di modello*, seleziona **Slack**.
4. Incolla l'URL sopra nel campo *URL*.

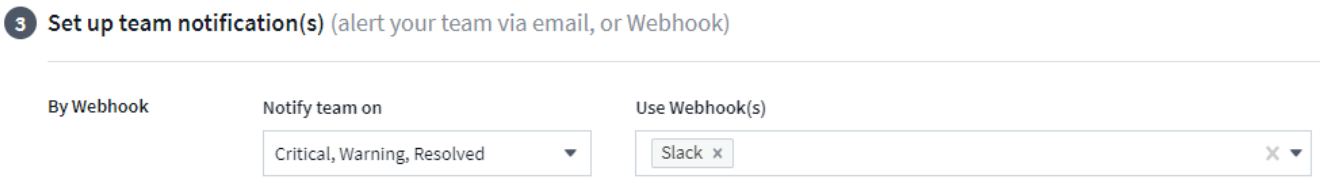


Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.

- Seleziona il webhook "Slack" per gli eventi desiderati (Critico, Avviso, Risolto)



Ulteriori informazioni:

- Per modificare il formato e il layout del messaggio, vedere https://api.slack.com/messaging/composing
- Gestione degli errori: https://api.slack.com/messaging/webhooks#handling_errors

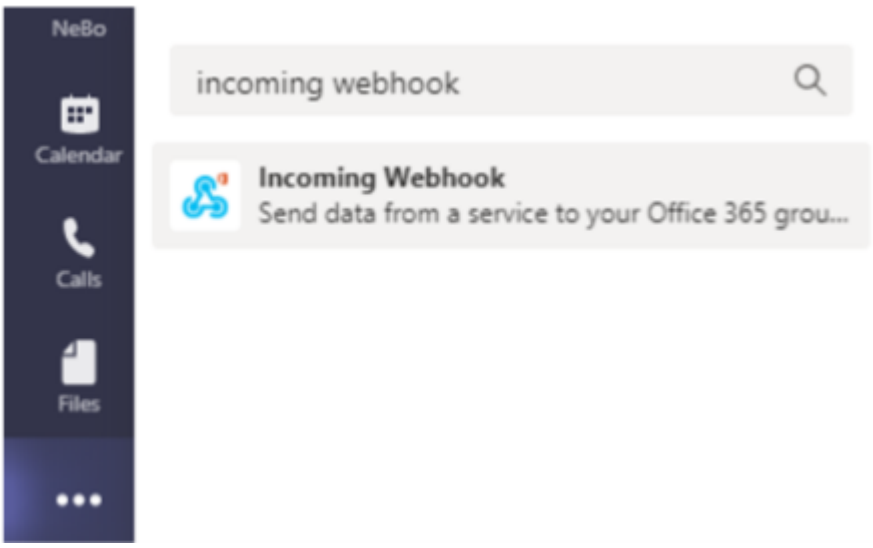
Esempio di webhook per Microsoft Teams

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per la configurazione di webhook per Teams.

Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione dei team" per le informazioni più aggiornate.

Configurazione delle squadre:

1. In Teams, seleziona il kebab e cerca Webhook in arrivo.

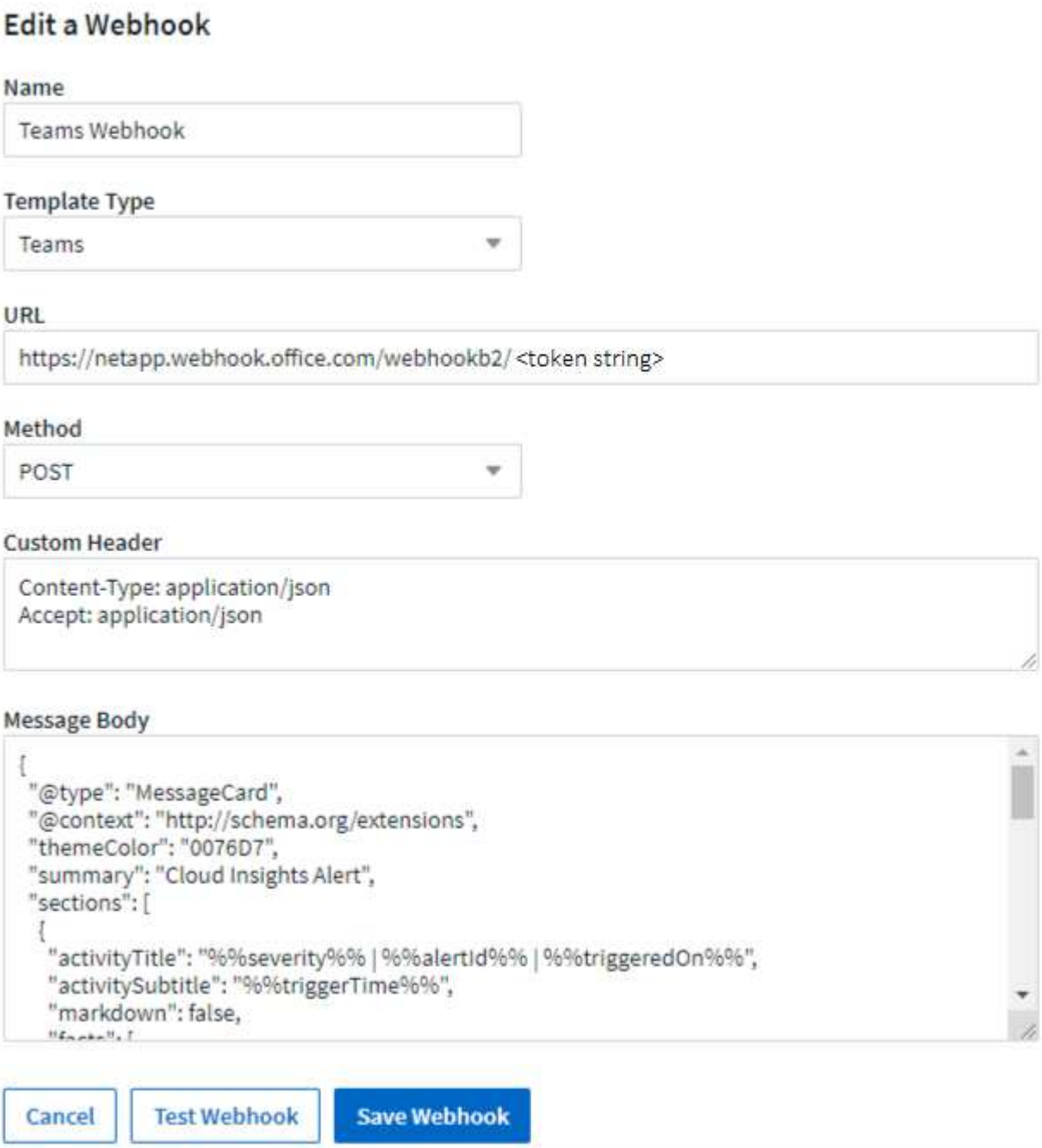


2. Seleziona **Aggiungi a un team > Seleziona un team > Imposta un connettore**.
3. Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Data Infrastructure Insights .

Crea un webhook Data Infrastructure Insights :

1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare clic su **+Webhook** per creare un nuovo webhook.

2. Assegna al webhook un nome significativo, ad esempio "Teams Webhook".
3. Nel menu a discesa *Tipo di modello*, seleziona **Team**.



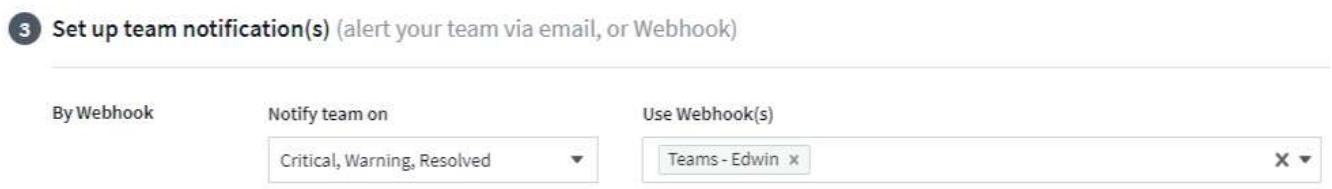
1. Incolla l'URL sopra nel campo *URL*.

Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.

- Seleziona il webhook "Team" per gli eventi desiderati (Critico, Avviso, Risolto)



Lavorare con le annotazioni

Definizione delle annotazioni

Quando si personalizza Data Infrastructure Insights per monitorare i dati in base alle esigenze aziendali, è possibile definire note specializzate, denominate annotazioni, e assegnarle alle risorse.

È possibile assegnare annotazioni alle risorse con informazioni quali fine del ciclo di vita della risorsa, data center, ubicazione dell'edificio, livello di archiviazione o livello di servizio del volume.

L'utilizzo delle annotazioni per monitorare l'ambiente include le seguenti attività di alto livello:

- Creazione o modifica di definizioni per tutti i tipi di annotazione.
- Visualizzazione delle pagine delle risorse e associazione di ciascuna risorsa a una o più annotazioni.

  Ad esempio, se un bene è in leasing e il leasing scade entro due mesi, potrebbe essere opportuno applicare un'annotazione di fine vita al bene. Ciò aiuta a impedire che altri utilizzino tale risorsa per un periodo di tempo prolungato.

- Creazione di regole per applicare automaticamente annotazioni a più risorse dello stesso tipo.
- Filtra le risorse in base alle loro annotazioni.

Tipi di annotazione predefiniti

Data Infrastructure Insights fornisce alcuni tipi di annotazione predefiniti. Queste annotazioni possono essere utilizzate per filtrare o raggruppare i dati.

È possibile associare le risorse a tipi di annotazione predefiniti come i seguenti:

- Ciclo di vita delle risorse, come compleanno, tramonto o fine vita
- Informazioni sulla posizione di un dispositivo, come centro dati, edificio o piano
- Classificazione delle risorse, ad esempio per qualità (livelli), per dispositivi connessi (livello di switch) o per livello di servizio
- Stato, ad esempio caldo (utilizzo elevato)

Nella tabella seguente sono elencati i tipi di annotazione forniti da Data Infrastructure Insights.

Tipi di annotazione	Descrizione	Tipo
Alias	Nome intuitivo per una risorsa	Testo

Gruppo di risorse di calcolo	Assegnazione di gruppo utilizzata dal raccoglitore dati dei file system host e VM	Lista
Centro dati	Posizione fisica	Lista
Caldo	Dispositivi sottoposti a un uso intenso su base regolare o al limite della capacità	Booleano
Nota	Commenti associati a una risorsa	Test
Livello di servizio	Un insieme di livelli di servizio supportati che è possibile assegnare alle risorse. Fornisce un elenco di opzioni ordinate per volumi interni, qtree e volumi. Modifica i livelli di servizio per impostare criteri di prestazione per livelli diversi.	Lista
Tramonto	Soglia impostata dopo la quale non è più possibile effettuare nuove allocazioni a quel dispositivo. Utile per migrazioni pianificate e altre modifiche di rete in sospeso.	Data
Cambia livello	Opzioni predefinite per l'impostazione delle categorie per gli switch. In genere, queste designazioni rimangono valide per tutta la vita del dispositivo, anche se è possibile modificarle. Disponibile solo per gli switch.	Lista
Livello	Può essere utilizzato per definire diversi livelli di servizio all'interno del tuo ambiente. I livelli possono definire il tipo di livello, ad esempio la velocità necessaria (ad esempio, oro o argento). Questa funzionalità è disponibile solo su volumi interni, qtree, array di archiviazione, pool di archiviazione e volumi.	Lista
Gravità della violazione	Grado (ad esempio, maggiore) di una violazione (ad esempio, porte host mancanti o ridondanza mancante), in una gerarchia dall'importanza più alta a quella più bassa.	Lista

Alias, Data Center, Hot, Service Level, Sunset, Switch Level, Tier e Violation Severity sono annotazioni a livello di sistema che non è possibile eliminare o rinominare; è possibile modificare solo i valori assegnati.

Creazione di annotazioni personalizzate

Utilizzando le annotazioni, puoi aggiungere alle risorse dati aziendali personalizzati e specifici che corrispondono alle tue esigenze aziendali. Sebbene Data Infrastructure Insights fornisca un set di annotazioni predefinite, potresti voler visualizzare i dati in altri modi. I dati nelle annotazioni personalizzate integrano i dati del dispositivo già raccolti, come il produttore dell'archiviazione, i volumi numerici e le statistiche sulle prestazioni. I dati aggiunti tramite annotazioni non vengono rilevati da Data Infrastructure Insights.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Gestisci > Annotazioni**.

   La pagina Annotazioni mostra l'elenco delle annotazioni.

2. Fai clic su **+Aggiungi**
3. Inserisci un **Nome** e una **Descrizione** dell'annotazione.

In questi campi è possibile immettere fino a 255 caratteri.

4. Fare clic su **Tipo** e quindi selezionare una delle seguenti opzioni che rappresenta il tipo di dati consentiti in questa annotazione:

Tipi di annotazione

- Booleano: crea un elenco a discesa con le opzioni Sì e No. Ad esempio, l'annotazione "Allegato diretto" è booleana.
- Data: crea un campo che contiene una data. Ad esempio, se l'annotazione sarà una data, selezionare questa opzione.
- Elenco: crea uno dei seguenti:
  - Un elenco fisso a discesa

    Quando altri assegnano questo tipo di annotazione su un dispositivo, non possono aggiungere altri valori all'elenco.

  - Un elenco flessibile a discesa

    Se selezioni l'opzione Aggiungi nuovi valori al volo quando crei questo elenco, quando altri assegnano questo tipo di annotazione su un dispositivo, possono aggiungere altri valori all'elenco.

- Numero: crea un campo in cui l'utente che assegna l'annotazione può immettere un numero. Ad esempio, se il tipo di annotazione è "Piano", l'utente può selezionare il tipo di valore "numero" e immettere il numero del piano.
- Testo: crea un campo che consente l'inserimento di testo libero. Ad esempio, potresti immettere "Lingua" come tipo di annotazione, selezionare "Testo" come tipo di valore e immettere una lingua come valore.

> Dopo aver impostato il tipo e salvato le modifiche, non è più possibile modificare il tipo di annotazione. Se è necessario modificare il tipo, è necessario eliminare l'annotazione e crearne una nuova.

1. Se selezioni Elenco come tipo di annotazione, procedi come segue:
   a. Seleziona **Aggiungi nuovi valori al volo** se desideri avere la possibilità di aggiungere più valori all'annotazione quando ti trovi su una pagina di risorse, creando un elenco flessibile.

      Ad esempio, supponiamo di trovarci su una pagina di risorse e che la risorsa abbia l'annotazione Città con i valori Detroit, Tampa e Boston. Se hai selezionato l'opzione **Aggiungi nuovi valori al volo**, puoi aggiungere valori aggiuntivi a città come San Francisco e Chicago direttamente nella pagina delle risorse, invece di dover andare alla pagina Annotazioni per aggiungerli. Se non si sceglie questa opzione, non sarà possibile aggiungere nuovi valori di annotazione quando si applica l'annotazione; ciò creerà un elenco fisso.

   b. Inserisci un valore e una descrizione nei campi **Valore** e **Descrizione**.
   c. Fare clic su **Aggiungi** per aggiungere altri valori.
   d. Fare clic sull'icona del cestino per eliminare un valore.
2. Fai clic su **Salva**

Le tue annotazioni vengono visualizzate nell'elenco nella pagina Annotazioni.

Una nota sulle annotazioni booleane

Quando si filtra un'annotazione booleana, potrebbero essere presentati i seguenti valori su cui filtrare:

- **Qualsiasi**: restituirà *tutti* i risultati, compresi i risultati impostati su "Sì", "No" o non impostati affatto.
- **Sì**: Restituisce solo risultati "Sì". Si noti che DII mostra "Sì" come segno di spunta nella maggior parte delle tabelle. I valori possono essere impostati su "True", "On", ecc.; DII li tratta tutti come "Sì".
- **No**: restituisce solo risultati "No". Si noti che DII mostra "No" come una "X" nella maggior parte delle tabelle. I valori possono essere impostati su "Falso", "Off", ecc.; DII li tratta tutti come "No".
- **Nessuno**: restituisce solo i risultati in cui l'annotazione non è stata impostata. Chiamati anche valori "Null".

Dopo aver finito

Nell'interfaccia utente, l'annotazione è immediatamente disponibile per l'uso.

Utilizzo delle annotazioni

Puoi creare annotazioni e assegnarle alle risorse che monitori. Le annotazioni sono note che forniscono informazioni su una risorsa, ad esempio la posizione fisica, la fine del ciclo di vita, il livello di archiviazione o i livelli di servizio del volume.

Definizione delle annotazioni

Utilizzando le annotazioni, puoi aggiungere alle risorse dati aziendali personalizzati e specifici che corrispondono alle tue esigenze aziendali. Sebbene Data Infrastructure Insights fornisca una serie di annotazioni predefinite, come il ciclo di vita delle risorse (data di nascita o fine vita), l'ubicazione dell'edificio o del data center e il livello, potresti voler visualizzare i dati in altri modi.

I dati nelle annotazioni personalizzate integrano i dati del dispositivo già raccolti, come il produttore dello switch, il numero di porte e le statistiche sulle prestazioni. I dati aggiunti tramite annotazioni non vengono rilevati da Data Infrastructure Insights.

Prima di iniziare

- Elencare qualsiasi terminologia del settore a cui devono essere associati i dati ambientali.
- Elencare la terminologia aziendale a cui devono essere associati i dati ambientali.
- Identifica i tipi di annotazione predefiniti che potresti essere in grado di utilizzare.
- Identifica quali annotazioni personalizzate devi creare. È necessario creare l'annotazione prima di poterla assegnare a una risorsa.

Per creare un'annotazione, attenersi alla seguente procedura.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Osservabilità > Arricchisci > Annotazioni**
2. Fare clic su **+ Annotazione** per creare una nuova annotazione.
3. Inserisci un nome, una descrizione e un tipo per la nuova annotazione.

   Ad esempio, immettere quanto segue per creare un'annotazione di testo che definisca la posizione fisica di una risorsa nel Data Center 4:

   - Inserisci un nome per l'annotazione, ad esempio "Posizione"
   - Inserisci una descrizione di ciò che l'annotazione descrive, ad esempio "La posizione fisica è il Data Center 4"

- Inserisci il "tipo" di annotazione, ad esempio "Testo".

Assegnazione manuale di annotazioni alle risorse

L'assegnazione di annotazioni alle risorse ti aiuta a ordinare, raggruppare e creare report sulle risorse in modi pertinenti alla tua attività. Sebbene sia possibile assegnare automaticamente annotazioni a risorse di un tipo specifico utilizzando le regole di annotazione, è possibile assegnare annotazioni a una singola risorsa utilizzando la relativa pagina delle risorse.

Prima di iniziare

- Devi aver creato l'annotazione che vuoi assegnare.

Passi

1. Accedi al tuo ambiente Data Infrastructure Insights .
2. Individua la risorsa a cui desideri applicare l'annotazione.
   - È possibile individuare le risorse tramite query, selezionandole da un widget del dashboard o tramite ricerca. Una volta individuata la risorsa desiderata, clicca sul link per aprire la landing page della risorsa.
3. Nella pagina delle risorse, nella sezione Dati utente, fare clic su **+ Annotazione**.
4. Viene visualizzata la finestra di dialogo Aggiungi annotazione.
5. Seleziona un'annotazione dall'elenco.
6. Fare clic su Valore ed effettuare una delle seguenti operazioni, a seconda del tipo di annotazione selezionato:
   - Se il tipo di annotazione è elenco, data o booleano, selezionare un valore dall'elenco.
   - Se il tipo di annotazione è testo, digitare un valore.
7. Fare clic su **Salva**.

Se si desidera modificare il valore dell'annotazione dopo averla assegnata, fare clic sul campo dell'annotazione e selezionare un valore diverso. Se l'annotazione è di tipo elenco per cui è selezionata l'opzione *Aggiungi nuovi valori al volo*, è possibile digitare un nuovo valore oltre a selezionare un valore esistente.

Assegnazione di annotazioni utilizzando le regole di annotazione

Per assegnare automaticamente annotazioni alle risorse in base ai criteri definiti, è possibile configurare le regole di annotazione. Data Infrastructure Insights assegna le annotazioni alle risorse in base a queste regole. Data Infrastructure Insights fornisce anche due regole di annotazione predefinite, che puoi modificare in base alle tue esigenze o rimuovere se non desideri utilizzarle.

Creazione di regole di annotazione

In alternativa all'applicazione manuale delle annotazioni alle singole risorse, è possibile applicare automaticamente le annotazioni a più risorse utilizzando le regole di annotazione. Le annotazioni impostate manualmente sulle singole pagine delle risorse hanno la precedenza sulle annotazioni basate su regole quando Insight valuta le regole di annotazione.

Prima di iniziare

Devi aver creato una query per la regola di annotazione.

Informazioni su questo compito

Sebbene sia possibile modificare i tipi di annotazione durante la creazione delle regole, è opportuno definire i tipi in anticipo.

Passi

1. Fare clic su **Gestisci > Regole di annotazione**

   La pagina Regole di annotazione visualizza l'elenco delle regole di annotazione esistenti.

2. Fare clic su **+ Aggiungi**.
3. Procedi come segue:
   a. Nella casella **Nome**, immettere un nome univoco che descriva la regola.

      Questo nome apparirà nella pagina Regole di annotazione.

   b. Fare clic su **Query** e selezionare la query utilizzata per applicare l'annotazione alle risorse.
   c. Fare clic su **Annotazione** e selezionare l'annotazione che si desidera applicare.
   d. Fare clic su **Valore** e selezionare un valore per l'annotazione.

      Ad esempio, se si sceglie Compleanno come annotazione, si specifica una data per il valore.

   e. Fai clic su **Salva**
   f. Fare clic su **Esegui tutte le regole** se si desidera eseguire tutte le regole immediatamente; in caso contrario, le regole vengono eseguite a intervalli regolari pianificati.

Creazione di regole di annotazione

È possibile utilizzare le regole di annotazione per applicare automaticamente annotazioni a più risorse in base ai criteri definiti. Data Infrastructure Insights assegna le annotazioni alle risorse in base a queste regole. Le annotazioni impostate manualmente sulle singole pagine delle risorse hanno la precedenza sulle annotazioni basate su regole quando Cloud Insight valuta le regole di annotazione.

Prima di iniziare

Devi aver creato una query per la regola di annotazione.

Passi

1. Nel menu Data Infrastructure Insights fare clic su **Gestisci > Regole di annotazione**.
2. Fare clic su **+ Regola** per aggiungere una nuova regola di annotazione.

   Viene visualizzata la finestra di dialogo Aggiungi regola.

3. Procedi come segue:
   a. Nella casella **Nome**, immettere un nome univoco che descriva la regola.

      Il nome appare nella pagina Regole di annotazione.

   b. Fare clic su **Query** e selezionare la query che Data Infrastructure Insights utilizza per identificare le risorse a cui si applica l'annotazione.
   c. Fare clic su **Annotazione** e selezionare l'annotazione che si desidera applicare.

d. Fare clic su **Valore** e selezionare un valore per l'annotazione.

   Ad esempio, se si sceglie Compleanno come annotazione, si specifica una data per il valore.

e. Fai clic su **Salva**

f. Fare clic su **Esegui tutte le regole** se si desidera eseguire tutte le regole immediatamente; in caso contrario, le regole vengono eseguite a intervalli regolari pianificati.

> In un ambiente Data Infrastructure Insights di grandi dimensioni, potresti notare che l'esecuzione delle regole di annotazione sembra richiedere un po' di tempo per essere completata. Ciò avviene perché l'indicizzatore viene eseguito per primo e deve essere completato prima di eseguire le regole. L'indicizzatore è ciò che consente a Data Infrastructure Insights di cercare o filtrare oggetti e contatori nuovi o aggiornati nei dati. Il motore delle regole attende che l'indicizzatore completi l'aggiornamento prima di applicare le regole.

Modifica delle regole di annotazione

È possibile modificare una regola di annotazione per cambiare il nome della regola, la sua annotazione, il valore dell'annotazione o la query associata alla regola.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Gestisci > Regole di annotazione**.

   La pagina Regole di annotazione visualizza l'elenco delle regole di annotazione esistenti.

2. Individua la regola di annotazione che desideri modificare.

   È possibile filtrare le regole di annotazione inserendo un valore nella casella del filtro oppure facendo clic su un numero di pagina per sfogliare le regole di annotazione per pagina.

3. Fare clic sull'icona del menu relativa alla regola che si desidera modificare.
4. Fai clic su **Modifica**

   Viene visualizzata la finestra di dialogo Modifica regola.

5. Modificare il nome, l'annotazione, il valore o la query della regola di annotazione.

Cambiare l'ordine delle regole

Le regole di annotazione vengono elaborate dall'alto verso il basso nell'elenco delle regole. Per modificare l'ordine in cui viene elaborata una regola, procedere come segue:

Passi

1. Fare clic sull'icona del menu relativa alla regola che si desidera spostare.
2. Fare clic su **Sposta su** o **Sposta giù**, a seconda delle necessità, finché la regola non viene visualizzata nella posizione desiderata.

Tieni presente che quando si eseguono più regole che aggiornano la stessa annotazione su una risorsa, la prima regola (eseguita dall'alto verso il basso) applica l'annotazione e aggiorna la risorsa, quindi si applica la seconda regola ma non modifica alcuna annotazione già impostata dalla regola precedente.

Eliminazione delle regole di annotazione

Potresti voler eliminare le regole di annotazione che non vengono più utilizzate.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Gestisci > Regole di annotazione**.

   La pagina Regole di annotazione visualizza l'elenco delle regole di annotazione esistenti.

2. Individua la regola di annotazione che desideri eliminare.

   È possibile filtrare le regole di annotazione inserendo un valore nella casella del filtro oppure facendo clic su un numero di pagina per sfogliare le regole di annotazione per pagina.

3. Fare clic sull'icona del menu relativa alla regola che si desidera eliminare.
4. Fai clic su **Elimina**

   Viene visualizzato un messaggio di conferma che chiede se si desidera eliminare la regola.

5. Fare clic su **OK**

Importazione di annotazioni

Data Infrastructure Insights include un'API per importare annotazioni o applicazioni da un file CSV e assegnarle agli oggetti specificati.

L'API Data Infrastructure Insights è disponibile nella * Data Infrastructure Insights Premium Edition*.

Importazione

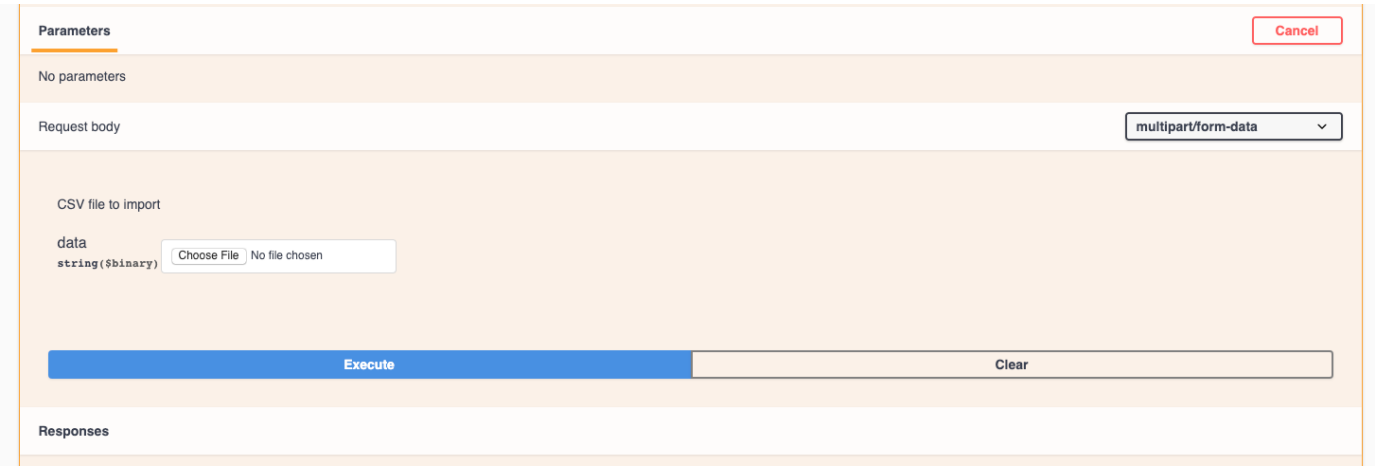
I link **Amministrazione > Accesso API** contengono"documentazione" per l'API **Risorse/Importazione**. Questa documentazione contiene informazioni sul formato file .CSV.

Formato file .CSV

Il formato generale del file CSV è il seguente. La prima riga del file definisce i campi di importazione e specifica l'ordine dei campi. Seguono righe separate per ogni annotazione o applicazione. Non è necessario definire ogni campo. Tuttavia, le righe di annotazione successive devono seguire lo stesso ordine della riga di definizione.

```
 [Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type,  ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
Per esempi di file .CSV, consultare la documentazione API.
```

È possibile importare e assegnare annotazioni da un file .CSV direttamente dall'API Swagger. Basta scegliere il file da utilizzare e cliccare sul pulsante *Esegui*:



Comportamento di importazione

Durante l'operazione di importazione, i dati vengono aggiunti, uniti o sostituiti, a seconda degli oggetti e dei tipi di oggetti che vengono importati. Durante l'importazione, tenere presente i seguenti comportamenti.

- Aggiunge un'annotazione o un'applicazione se non ne esiste nessuna con lo stesso nome nel sistema di destinazione.
- Unisce un'annotazione se il tipo di annotazione è un elenco e nel sistema di destinazione esiste un'annotazione con lo stesso nome.
- Sostituisce un'annotazione se il tipo di annotazione è diverso da un elenco e nel sistema di destinazione esiste un'annotazione con lo stesso nome.

  Nota: se nel sistema di destinazione esiste un'annotazione con lo stesso nome ma con un tipo diverso, l'importazione fallisce. Se gli oggetti dipendono dall'annotazione non riuscita, tali oggetti potrebbero mostrare informazioni errate o indesiderate. Dopo aver completato l'operazione di importazione, è necessario controllare tutte le dipendenze delle annotazioni.

- Se un valore di annotazione è vuoto, l'annotazione viene rimossa dall'oggetto. Le annotazioni ereditate non sono interessate.
- I valori di annotazione del tipo data devono essere passati come tempo Unix in millisecondi.
- Quando si annotano volumi o volumi interni, il nome dell'oggetto è una combinazione del nome di archiviazione e del nome del volume utilizzando il separatore "->". Ad esempio: *<Nome archivio>-><Nome volume>*
- Se il nome di un oggetto contiene una virgola, l'intero nome deve essere racchiuso tra virgolette doppie. Ad esempio: *"NetApp1,NetApp2"->023F*
- Quando si associano annotazioni a storage, switch e porte, la colonna "Applicazione" verrà ignorata.

- Tenant, Line_Of_Business, Business_Unit e/o Project costituiscono un'entità aziendale. Come per tutte le entità aziendali, qualsiasi valore può essere vuoto.

È possibile annotare i seguenti tipi di oggetti.

TIPO DI OGGETTO	NOME O CHIAVE
Ospite	id-><id> o <Nome> o <IP>
Macchina virtuale	id-><id> o <Nome>
StoragePool	id-><id> o <Nome archivio>-><Nome pool di archiviazione>
Volume interno	id-><id> o <Nome archivio>-><Nome volume interno>
Volume	id-><id> o <Nome archivio>-><Nome volume>
Magazzinaggio	id-><id> o <Nome> o <IP>
Interruttore	id-><id> o <Nome> o <IP>
Porta	id-><id> o <WWN>
Qtree	id-><id> o <Nome archivio>-><Nome volume interno>-><Nome Qtree>
Condividere	id-><id> o <Nome archivio>-><Nome volume interno>-><Nome condivisione>-><Protocollo>[-><Nome Qtree (facoltativo in caso di Qtree predefinito)>]

Lavorare con le applicazioni

Monitoraggio dell'utilizzo delle risorse per applicazione

Conoscere le applicazioni utilizzate nell'ambiente aziendale aiuta a tenere traccia dell'utilizzo e dei costi delle risorse.

Prima di poter monitorare i dati associati alle applicazioni in esecuzione sul tenant, è necessario definire tali applicazioni e associarle alle risorse appropriate. È possibile associare le applicazioni alle seguenti risorse: host, macchine virtuali, volumi, volumi interni, qtree, condivisioni e hypervisor.

Questo argomento fornisce un esempio di monitoraggio dell'utilizzo delle macchine virtuali utilizzate dal team di marketing per la posta elettronica di Exchange.

Potresti voler creare una tabella simile alla seguente per identificare le applicazioni utilizzate sul tuo tenant e annotare il gruppo o l'unità aziendale che utilizza ciascuna applicazione.

Inquilino	Linea di business	Unità aziendale	Progetto	Applicazioni
NetApp	Archiviazione dati	Legal	Brevetti	Oracle Identity Manager, Oracle On Demand, PatentWiz

NetApp	Archiviazione dati	Marketing	Eventi di vendita	Exchange, Oracle Shared Database, BlastOff Event Planner

La tabella mostra che il team di marketing utilizza l'applicazione Exchange. Vogliamo monitorare l'utilizzo delle loro macchine virtuali per Exchange, in modo da poter prevedere quando sarà necessario aggiungere altro spazio di archiviazione. Possiamo associare l'applicazione Exchange a tutte le macchine virtuali di Marketing:

1. Crea un'applicazione denominata *Exchange*
2. Vai su **Query > +Nuova query** per creare una nuova query per le macchine virtuali (oppure seleziona una query VM esistente, se applicabile).

   Supponendo che tutte le VM del team di marketing abbiano un nome contenente la stringa "**mkt**", crea la tua query per filtrare il nome della VM per "mkt".

3. Selezionare le VM.
4. Associare le VM all'applicazione *Exchange* utilizzando **Azioni in blocco > Aggiungi applicazioni**.
5. Selezionare l'applicazione desiderata e fare clic su **Salva**.
6. Al termine, **Salva** la query.

Creazione di applicazioni

Per tenere traccia dei dati associati ad applicazioni specifiche in esecuzione sul tuo tenant, puoi definire le applicazioni in Data Infrastructure Insights.

Informazioni su questo compito

Data Infrastructure Insights consente di monitorare i dati provenienti dalle risorse associate alle applicazioni per scopi quali la rendicontazione dell'utilizzo o dei costi.

Passi

1. Nel menu Data Infrastructure Insights , fare clic su **Osservabilità > Arricchisci > Applicazioni**. Selezionare

   Viene visualizzata la finestra di dialogo Aggiungi applicazione.

2. Inserisci un nome univoco per l'applicazione.
3. Seleziona una priorità per l'applicazione.
4. Fare clic su **Salva**.

Dopo aver definito un'applicazione, è possibile assegnarla alle risorse.

Assegnazione delle applicazioni alle risorse

Questa procedura assegna l'applicazione a un host come esempio. È possibile assegnare host, macchine virtuali, volumi o volumi interni a un'applicazione.

Passi

1. Individua la risorsa a cui vuoi assegnare l'applicazione:

2. Fare clic su **Query > +Nuova query** e cercare Host.
3. Fare clic sulla casella di controllo a sinistra dell'host che si desidera associare all'applicazione.
4. Fare clic su **Azioni in blocco > Aggiungi applicazione**.
5. Seleziona l'applicazione a cui vuoi assegnare la risorsa.

Tutte le nuove applicazioni assegnate sovrascrivono tutte le applicazioni sulla risorsa derivate da un'altra risorsa. Ad esempio, i volumi ereditano le applicazioni dagli host e quando a un volume vengono assegnate nuove applicazioni, la nuova applicazione ha la precedenza sull'applicazione derivata.

Per ambienti con grandi quantità di risorse correlate, l'ereditarietà delle assegnazioni delle applicazioni a tali risorse potrebbe richiedere diversi minuti. Se si hanno molti beni correlati, si prega di attendere più tempo affinché l'eredità avvenga.

Dopo aver finito

Dopo aver assegnato l'host all'applicazione, è possibile assegnare le risorse rimanenti all'applicazione. Per accedere alla landing page dell'applicazione, clicca su **Gestisci > Applicazione** e seleziona l'applicazione che hai creato.

Risoluzione automatica del dispositivo

Panoramica sulla risoluzione automatica del dispositivo

È necessario identificare tutti i dispositivi che si desidera monitorare con Data Infrastructure Insights. L'identificazione è necessaria per monitorare con precisione le prestazioni e l'inventario del tuo inquilino. In genere la maggior parte dei dispositivi rilevati nel tenant vengono identificati tramite la *Risoluzione automatica dei dispositivi*.

Dopo aver configurato i data collector, vengono identificati i dispositivi sul tenant, inclusi switch, array di archiviazione e l'infrastruttura virtuale di hypervisor e VM. Tuttavia, questo non consente di identificare normalmente il 100% dei dispositivi presenti nel tenant.

Dopo aver configurato i dispositivi di tipo raccoglitore dati, la procedura consigliata è quella di sfruttare le regole di risoluzione dei dispositivi per identificare i dispositivi sconosciuti rimanenti nel tenant. La risoluzione dei dispositivi può aiutarti a distinguere i dispositivi sconosciuti dai seguenti tipi di dispositivi:

- Host fisici
- Array di archiviazione
- Nastri

I dispositivi che rimangono sconosciuti dopo la risoluzione sono considerati dispositivi generici e possono essere visualizzati anche nelle query e nelle dashboard.

Le regole create a loro volta identificheranno automaticamente i nuovi dispositivi con attributi simili man mano che vengono aggiunti al tuo ambiente. In alcuni casi, la risoluzione del dispositivo consente anche l'identificazione manuale, bypassando le regole di risoluzione del dispositivo per i dispositivi non rilevati in Data Infrastructure Insights.

L'identificazione incompleta dei dispositivi può comportare problemi tra cui:

- Percorsi incompleti

- Connessioni multipath non identificate
- L’impossibilità di raggruppare le applicazioni
- Viste topologiche imprecise
- Dati imprecisi nel data warehouse e nel reporting

La funzionalità di risoluzione del dispositivo (Gestisci > Risoluzione del dispositivo) include le seguenti schede, ciascuna delle quali svolge un ruolo nella pianificazione della risoluzione del dispositivo e nella visualizzazione dei risultati:

- **Fibre Channel Identify** contiene un elenco di WWN e informazioni sulle porte dei dispositivi Fibre Channel che non sono stati risolti tramite la risoluzione automatica dei dispositivi. Nella scheda è indicata anche la percentuale di dispositivi identificati.
- **Identificazione indirizzo IP** contiene un elenco dei dispositivi che accedono alle condivisioni CIFS e NFS che non sono stati identificati tramite la risoluzione automatica dei dispositivi. Nella scheda è indicata anche la percentuale di dispositivi identificati.
- **Regole di risoluzione automatica** contiene l’elenco delle regole eseguite durante la risoluzione del dispositivo Fibre Channel. Si tratta di regole create per risolvere i problemi relativi ai dispositivi Fibre Channel non identificati.
- **Preferenze** fornisce opzioni di configurazione che puoi utilizzare per personalizzare la risoluzione del dispositivo in base al tuo ambiente.

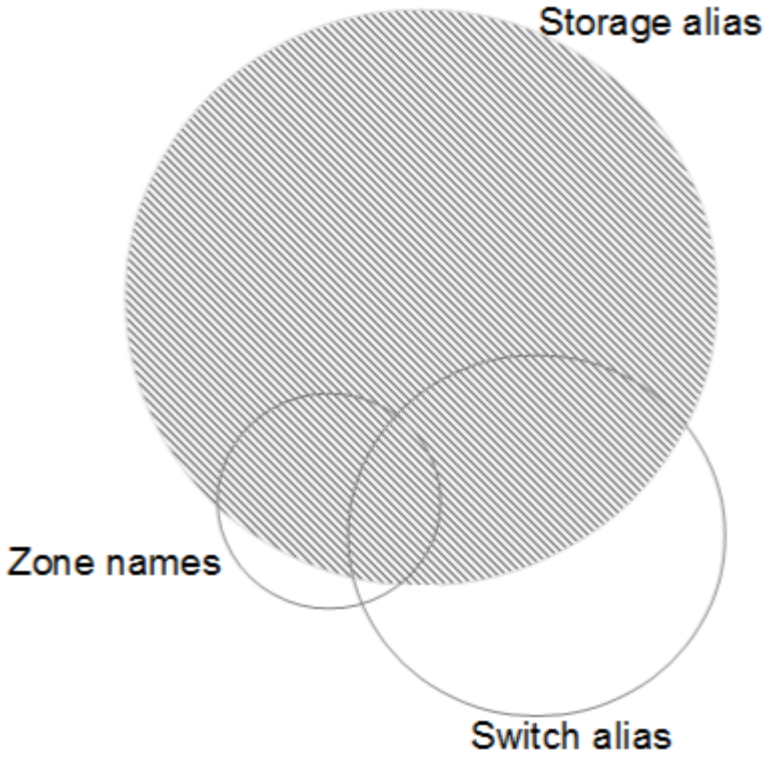
Prima di iniziare

Prima di definire le regole per l’identificazione dei dispositivi, è necessario sapere come è configurato il proprio ambiente. Quanto più conosci l’ambiente circostante, tanto più facile sarà identificare i dispositivi.

Per creare regole precise, è necessario rispondere a domande simili alle seguenti:

- Il tuo ambiente ha standard di denominazione per zone o host e quale percentuale di questi è accurata?
- Il tuo ambiente utilizza un alias di switch o di storage e questi corrispondono al nome host?
- Con quale frequenza cambiano gli schemi di denominazione del tuo tenant?
- Ci sono state acquisizioni o fusioni che hanno introdotto schemi di denominazione diversi?

Dopo aver analizzato il tuo ambiente, dovresti essere in grado di identificare quali standard di denominazione esistono che puoi aspettarti di incontrare in termini di affidabilità. Le informazioni raccolte potrebbero essere rappresentate graficamente in una figura simile alla seguente:



In questo esempio il maggior numero di dispositivi è rappresentato in modo affidabile da alias di archiviazione. Le regole che identificano gli host utilizzando alias di archiviazione devono essere scritte per prime, le regole che utilizzano alias di switch devono essere scritte successivamente e le ultime regole create devono utilizzare alias di zona. A causa della sovrapposizione dell'uso di alias di zona e alias di switch, alcune regole di alias di archiviazione potrebbero identificare dispositivi aggiuntivi, lasciando meno regole necessarie per alias di zona e alias di switch.

Passaggi per l'identificazione dei dispositivi

In genere, per identificare i dispositivi nel tenant si utilizza un flusso di lavoro simile al seguente. L'identificazione è un processo iterativo e potrebbe richiedere più fasi di pianificazione e perfezionamento delle regole.

- Ambiente di ricerca
- Regole del piano
- Crea/Revisiona regole
- Risultati della revisione
- Crea regole aggiuntive o identifica manualmente i dispositivi
- Fatto

Se nel tenant sono presenti dispositivi non identificati (altrimenti noti come dispositivi sconosciuti o generici) e successivamente si configura un'origine dati che identifica tali dispositivi durante l'interrogazione, questi non verranno più visualizzati o conteggiati come dispositivi generici.

Imparentato:"Creazione di regole di risoluzione del dispositivo" "Risoluzione del dispositivo Fibre Channel" "Risoluzione del dispositivo IP" "Impostazione delle preferenze di risoluzione del dispositivo"

Regole di risoluzione del dispositivo

È possibile creare regole di risoluzione dei dispositivi per identificare host, storage e nastri che attualmente non vengono identificati automaticamente da Data Infrastructure Insights. Le regole create identificano i dispositivi attualmente presenti nel tuo ambiente e identificano anche i dispositivi simili man mano che vengono aggiunti al tuo ambiente.

Creazione di regole di risoluzione del dispositivo

Quando si creano regole, si inizia identificando la fonte delle informazioni su cui viene eseguita la regola, il metodo utilizzato per estrarre le informazioni e se la ricerca DNS viene applicata ai risultati della regola.

Fonte utilizzata per identificare il dispositivo	* Alias SRM per gli host * Alias di archiviazione contenente un nome host o nastro incorporato * Alias di switch contenente un nome host o nastro incorporato * Nomi di zona contenenti un nome host incorporato
Metodo utilizzato per estrarre il nome del dispositivo dalla sorgente	* Così com'è (estrae un nome da un SRM) * Delimitatori * Espressioni regolari
Ricerca DNS	Specifica se si utilizza DNS per verificare il nome host

È possibile creare regole nella scheda Regole di risoluzione automatica. I passaggi seguenti descrivono il processo di creazione delle regole.

Procedura

1. Fare clic su **Gestisci > Risoluzione dispositivo**
2. Nella scheda **Regole di risoluzione automatica**, fare clic su **+ Regola host** o **+ Regola nastro**.

   Viene visualizzata la schermata **Regola di risoluzione**.

   Fare clic sul collegamento *Visualizza criteri di corrispondenza* per ottenere assistenza ed esempi sulla creazione di espressioni regolari.

3. Nell'elenco **Tipo** seleziona il dispositivo che vuoi identificare.

   È possibile selezionare *Host* o *Tape*.

4. Nell'elenco **Origine**, seleziona la sorgente che desideri utilizzare per identificare l'host.

   A seconda della fonte scelta, Data Infrastructure Insights visualizza la seguente risposta:

   a. **Zone** elenca le zone e i WWN che devono essere identificati da Data Infrastructure Insights.
   b. **SRM** elenca gli alias non identificati che devono essere identificati da Data Infrastructure Insights
   c. **Alias di archiviazione** elenca gli alias di archiviazione e WWN che devono essere identificati da Data Infrastructure Insights
   d. **Alias dello switch** elenca gli alias dello switch che devono essere identificati da Data Infrastructure Insights

5. Nell'elenco **Metodo** seleziona il metodo che desideri utilizzare per identificare l'host.

Fonte	Metodo
SRM	Così com'è, Delimitatori, Espressioni regolari
Alias di archiviazione	Delimitatori, espressioni regolari
Cambia alias	Delimitatori, espressioni regolari
Zone	Delimitatori, espressioni regolari

- Le regole che utilizzano i delimitatori richiedono i delimitatori e la lunghezza minima del nome host. La lunghezza minima del nome host è il numero di caratteri che Data Infrastructure Insights deve utilizzare per identificare un host. Data Infrastructure Insights esegue ricerche DNS solo per nomi host di questa lunghezza o più lunghi.

  Per le regole che utilizzano i delimitatori, la stringa di input viene tokenizzata dal delimitatore e viene creato un elenco di nomi host candidati eseguendo diverse combinazioni del token adiacente. L'elenco viene quindi ordinato dal più grande al più piccolo. Ad esempio, per una sorgente di input di *vipsnq03_hba3_emc3_12ep0* l'elenco produrrebbe il seguente risultato:

  - vipsnq03_hba3_emc3_12ep0
  - vipsnq03_hba3_emc3
  - hba3 emc3_12ep0
  - vipsnq03_hba3
  - emc3_12ep0
  - hba3_emc3
  - vipsnq03
  - 12ep0
  - emc3
  - hba3
- Le regole che utilizzano espressioni regolari richiedono un'espressione regolare, il formato e la selezione della distinzione tra maiuscole e minuscole.

6. Fare clic su **Esegui AR** per eseguire tutte le regole oppure fare clic sulla freccia rivolta verso il basso nel pulsante per eseguire la regola creata (e tutte le altre regole create dall'ultima esecuzione completa di AR).

   I risultati dell'esecuzione della regola vengono visualizzati nella scheda **Identificazione FC**.

Avvio di un aggiornamento automatico della risoluzione del dispositivo

Un aggiornamento della risoluzione del dispositivo conferma le modifiche manuali aggiunte dall'ultima esecuzione completa della risoluzione automatica del dispositivo. L'esecuzione di un aggiornamento può essere utilizzata per confermare ed eseguire solo le nuove voci manuali apportate alla configurazione della risoluzione del dispositivo. Non viene eseguita alcuna risoluzione completa del dispositivo.

Procedura

1. Accedi all'interfaccia utente web Data Infrastructure Insights .
2. Fare clic su **Gestisci > Risoluzione dispositivo**
3. Nella schermata **Risoluzione dispositivo**, fare clic sulla freccia rivolta verso il basso nel pulsante **Esegui AR**.

4. Fare clic su **Aggiorna** per avviare l'aggiornamento.

Identificazione manuale assistita da regole

Questa funzionalità viene utilizzata in casi speciali in cui si desidera eseguire una regola specifica o un elenco di regole (con o senza un riordino una tantum) per risolvere host, dispositivi di archiviazione e dispositivi a nastro sconosciuti.

Prima di iniziare

Ci sono diversi dispositivi che non sono stati identificati e ci sono anche più regole che hanno identificato correttamente altri dispositivi.

> Se la sorgente contiene solo una parte del nome di un host o di un dispositivo, utilizzare una regola di espressione regolare e formattarla per aggiungere il testo mancante.

Procedura

1. Accedi all'interfaccia utente web Data Infrastructure Insights .
2. Fare clic su **Gestisci > Risoluzione dispositivo**
3. Fare clic sulla scheda **Identificazione Fibre Channel**.

   Il sistema visualizza i dispositivi insieme al loro stato di risoluzione.

4. Seleziona più dispositivi non identificati.
5. Fare clic su **Azioni in blocco** e selezionare **Imposta risoluzione host** o **Imposta risoluzione nastro**.

   Il sistema visualizza la schermata Identifica, che contiene un elenco di tutte le regole che hanno identificato correttamente i dispositivi.

6. Modifica l'ordine delle regole in base alle tue esigenze.

   L'ordine delle regole viene modificato nella schermata Identifica, ma non a livello globale.

7. Seleziona il metodo che soddisfa le tue esigenze.

Data Infrastructure Insights esegue il processo di risoluzione dell'host nell'ordine in cui compaiono i metodi, iniziando da quelli in alto.

Quando vengono rilevate delle regole applicabili, i nomi delle regole vengono visualizzati nella colonna delle regole e identificati come manuali.

Imparentato:"Risoluzione del dispositivo Fibre Channel" "Risoluzione del dispositivo IP" "Impostazione delle preferenze di risoluzione del dispositivo"

Risoluzione del dispositivo Fibre Channel

La schermata Identificazione Fibre Channel visualizza il WWN e il WWPN dei dispositivi Fibre Channel i cui host non sono stati identificati dalla risoluzione automatica dei dispositivi. Nella schermata vengono inoltre visualizzati tutti i dispositivi che sono stati risolti manualmente.

I dispositivi che sono stati risolti tramite risoluzione manuale contengono lo stato *OK* e identificano la regola utilizzata per identificare il dispositivo. I dispositivi mancanti hanno lo stato *Non identificato*. I dispositivi

specificatamente esclusi dall'identificazione hanno lo stato *Escluso*. La copertura totale per l'identificazione dei dispositivi è elencata in questa pagina.

È possibile eseguire azioni in blocco selezionando più dispositivi sul lato sinistro della schermata Identificazione Fibre Channel. È possibile eseguire azioni su un singolo dispositivo passando il mouse sopra il dispositivo e selezionando i pulsanti *Identifica* o *Annulla identificazione* all'estrema destra dell'elenco.

Il collegamento *Copertura totale* visualizza un elenco del numero di dispositivi identificati/numero di dispositivi disponibili per la configurazione:

- Alias SRM
- Alias di archiviazione
- Cambia alias
- Zone
- Definito dall'utente

Aggiunta manuale di un dispositivo Fibre Channel

È possibile aggiungere manualmente un dispositivo Fibre Channel a Data Infrastructure Insights utilizzando la funzionalità *Aggiunta manuale* disponibile nella scheda Identificazione Fibre Channel della risoluzione del dispositivo. Questo processo potrebbe essere utilizzato per la pre-identificazione di un dispositivo che si prevede di scoprire in futuro.

Prima di iniziare

Per aggiungere correttamente l'identificazione di un dispositivo al sistema è necessario conoscere l'indirizzo WWN o IP e il nome del dispositivo.

Informazioni su questo compito

È possibile aggiungere manualmente un dispositivo host, storage, tape o fibre channel sconosciuto.

Procedura

1. Accedi all'interfaccia utente web Data Infrastructure Insights
2. Fare clic su **Gestisci > Risoluzione dispositivo**
3. Fare clic sulla scheda **Identificazione Fibre Channel**.
4. Fare clic sul pulsante **Aggiungi**.

   Viene visualizzata la finestra di dialogo **Aggiungi dispositivo**

5. Inserisci l'indirizzo WWN o IP, il nome del dispositivo e seleziona il tipo di dispositivo.

   Il dispositivo immesso viene aggiunto all'elenco dei dispositivi nella scheda Identificazione Fibre Channel. La regola è identificata come *Manuale*.

Importazione dell'identificazione del dispositivo Fibre Channel da un file .CSV

È possibile importare manualmente l'identificazione del dispositivo Fibre Channel nella risoluzione dei dispositivi Data Infrastructure Insights utilizzando un elenco di dispositivi in un file .CSV.

1. Prima di iniziare

Per importare le identificazioni dei dispositivi direttamente nella risoluzione dei dispositivi, è necessario

disporre di un file .CSV formattato correttamente. Il file .CSV per i dispositivi Fibre Channel richiede le seguenti informazioni:

WWN	Proprietà intellettuale	Nome	Tipo

I campi dati devono essere racchiusi tra virgolette, come mostrato nell'esempio seguente.

```
"WWN","IP","Name","Type"
"WWN:2693","ADDRESS2693|IP2693","NAME-2693","HOST"
"WWN:997","ADDRESS997|IP997","NAME-997","HOST"
"WWN:1860","ADDRESS1860|IP1860","NAME-1860","HOST"
```

Come buona pratica, si consiglia di esportare prima le informazioni di Fibre Channel Identify in un file .CSV, apportare le modifiche desiderate in tale file e quindi importare nuovamente il file in Fibre Channel Identify. Ciò garantisce che le colonne previste siano presenti e nell'ordine corretto.

Per importare le informazioni di identificazione del Fibre Channel:

1. Accedi all'interfaccia utente web Data Infrastructure Insights .
2. Fare clic su **Gestisci > Risoluzione dispositivo**
3. Selezionare la scheda **Identificazione Fibre Channel**.
4. Fare clic sul pulsante **Identifica > Identifica dal file**.
5. Vai alla cartella contenente i file .CSV da importare e seleziona il file desiderato.

   I dispositivi immessi vengono aggiunti all'elenco dei dispositivi nella scheda Identificazione Fibre Channel. La "Regola" è identificata come Manuale.

Esportazione delle identificazioni dei dispositivi Fibre Channel in un file .CSV

È possibile esportare le identificazioni dei dispositivi Fibre Channel esistenti in un file .CSV dalla funzionalità di risoluzione dei dispositivi Data Infrastructure Insights . Potresti voler esportare l'identificazione di un dispositivo in modo da poterla modificare e poi importarla nuovamente in Data Infrastructure Insights, dove verrà utilizzata per identificare dispositivi simili a quelli che originariamente corrispondevano all'identificazione esportata.

Informazioni su questo compito

Questo scenario potrebbe essere utilizzato quando i dispositivi hanno attributi simili che possono essere facilmente modificati nel file .CSV e quindi importati nuovamente nel sistema.

Quando si esporta l'identificazione di un dispositivo Fibre Channel in un file .CSV, il file contiene le seguenti informazioni nell'ordine mostrato:

WWN	Proprietà intellettuale	Nome	Tipo

Procedura

1. Accedi all'interfaccia utente web Data Infrastructure Insights .
2. Fare clic su **Gestisci > Risoluzione dispositivo**

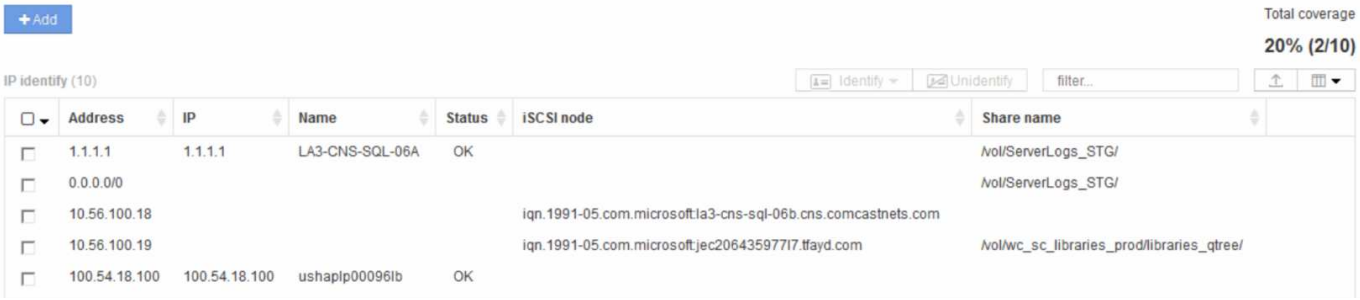
3. Selezionare la scheda **Identificazione Fibre Channel**.
4. Selezionare il dispositivo o i dispositivi Fibre Channel di cui si desidera esportare l'identificazione.
5. Fare clic su *Esporta* pulsante.

   Selezionare se aprire il file .CSV o salvarlo.

Imparentato:"Risoluzione del dispositivo IP" "Creazione di regole di risoluzione del dispositivo" "Impostazione delle preferenze di risoluzione del dispositivo"

Risoluzione del dispositivo IP

Nella schermata Identificazione IP vengono visualizzate tutte le condivisioni iSCSI e CIFS o NFS identificate tramite risoluzione automatica del dispositivo o tramite risoluzione manuale del dispositivo. Sono mostrati anche dispositivi non identificati. La schermata include l'indirizzo IP, il nome, lo stato, il nodo iSCSI e il nome di condivisione per i dispositivi. Viene visualizzata anche la percentuale di dispositivi identificati correttamente.



Aggiunta manuale di dispositivi IP

È possibile aggiungere manualmente un dispositivo IP a Data Infrastructure Insights utilizzando la funzionalità di aggiunta manuale disponibile nella schermata Identificazione IP.

Procedura

1. Accedi all'interfaccia utente web Data Infrastructure Insights .
2. Fare clic su **Gestisci > Risoluzione dispositivo**
3. Fare clic sulla scheda **Identificazione indirizzo IP**.
4. Fare clic sul pulsante **Aggiungi**.

   Viene visualizzata la finestra di dialogo Aggiungi dispositivo

5. Inserisci l'indirizzo, l'indirizzo IP e un nome univoco per il dispositivo.

Risultato

Il dispositivo immesso viene aggiunto all'elenco dei dispositivi nella scheda Identificazione indirizzo IP.

Importazione dell'identificazione del dispositivo IP da un file .CSV

È possibile importare manualmente le identificazioni dei dispositivi IP nella funzionalità Risoluzione dispositivi utilizzando un elenco di identificazioni dei dispositivi in un file .CSV.

1. Prima di iniziare

Per importare le identificazioni dei dispositivi direttamente nella funzionalità Risoluzione dispositivi, è necessario disporre di un file .CSV formattato correttamente. Il file .CSV per i dispositivi IP richiede le seguenti informazioni:

Indirizzo	Proprietà intellettuale	Nome

I campi dati devono essere racchiusi tra virgolette, come mostrato nell'esempio seguente.

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

Come buona pratica, si consiglia di esportare prima le informazioni di identificazione dell'indirizzo IP in un file .CSV, apportare le modifiche desiderate in tale file e quindi importare nuovamente il file in IP Address Identify. Ciò garantisce che le colonne previste siano presenti e nell'ordine corretto.

Esportazione dell'identificazione del dispositivo IP in un file .CSV

È possibile esportare le identificazioni dei dispositivi IP esistenti in un file .CSV dalla funzionalità di risoluzione dei dispositivi Data Infrastructure Insights . Potresti voler esportare l'identificazione di un dispositivo in modo da poterla modificare e poi importarla nuovamente in Data Infrastructure Insights, dove verrà utilizzata per identificare dispositivi simili a quelli che originariamente corrispondevano all'identificazione esportata.

Informazioni su questo compito

1. Questo scenario potrebbe essere utilizzato quando i dispositivi hanno attributi simili che possono essere facilmente modificati nel file .CSV e quindi importati nuovamente nel sistema.

Quando si esporta l'identificazione di un dispositivo IP in un file .CSV, il file contiene le seguenti informazioni nell'ordine mostrato:

Indirizzo	Proprietà intellettuale	Nome

Procedura

1. Accedi all'interfaccia utente web Data Infrastructure Insights .
2. Fare clic su **Gestisci > Risoluzione dispositivo**
3. Selezionare la scheda **Identificazione indirizzo IP**.
4. Selezionare il dispositivo o i dispositivi IP di cui si desidera esportare l'identificazione.
5. Fare clic su *Esporta* pulsante.

   Selezionare se aprire il file .CSV o salvarlo.

Imparentato:"Risoluzione del dispositivo Fibre Channel" "Creazione di regole di risoluzione del dispositivo" "Impostazione delle preferenze di risoluzione del dispositivo"

Impostazione delle opzioni nella scheda Preferenze

La scheda delle preferenze di risoluzione del dispositivo consente di creare una pianificazione di risoluzione automatica, specificare i fornitori di storage e nastri da includere o escludere dall'identificazione e impostare le opzioni di ricerca DNS.

Pianificazione della risoluzione automatica

Una pianificazione di risoluzione automatica può specificare quando eseguire la risoluzione automatica del dispositivo:

Opzione	Descrizione
Ogni	Utilizzare questa opzione per eseguire la risoluzione automatica del dispositivo a intervalli di giorni, ore o minuti.
Ogni giorno	Utilizzare questa opzione per eseguire la risoluzione automatica del dispositivo ogni giorno a un orario specifico.
Manualmente	Utilizzare questa opzione per eseguire manualmente solo la risoluzione automatica del dispositivo.
Ad ogni cambiamento ambientale	Utilizzare questa opzione per eseguire la risoluzione automatica del dispositivo ogni volta che si verifica una modifica nell'ambiente.

Se si specifica *Manualmente*, la risoluzione automatica notturna del dispositivo è disabilitata.

Opzioni di elaborazione DNS

Le opzioni di elaborazione DNS consentono di selezionare le seguenti funzionalità:

- Quando l'elaborazione dei risultati della ricerca DNS è abilitata, è possibile aggiungere un elenco di nomi DNS da aggiungere ai dispositivi risolti.
- È possibile selezionare Risoluzione automatica degli IP: per abilitare la risoluzione automatica degli host per gli iniziatori iSCSI e gli host che accedono alle condivisioni NFS tramite la ricerca DNS. Se non viene specificato, viene eseguita solo la risoluzione basata su FC.
- È possibile scegliere di consentire i caratteri di sottolineatura nei nomi host e di utilizzare un alias "connesso a" anziché l'alias di porta standard nei risultati.

Inclusione o esclusione di specifici fornitori di storage e nastri

È possibile includere o escludere specifici fornitori di storage e nastri per la risoluzione automatica. Potresti voler escludere fornitori specifici se sai, ad esempio, che un host specifico diventerà un host legacy e dovrà essere escluso dal tuo nuovo ambiente. Puoi anche aggiungere nuovamente i fornitori che hai escluso in precedenza ma che non desideri più escludere.

Le regole di risoluzione del dispositivo per il nastro funzionano solo per i WWN in cui il fornitore per quel WWN è impostato su *Incluso solo come nastro* nelle preferenze del fornitore.

Vedi anche:"Esempi di espressioni regolari"

Esempi di espressioni regolari

Se hai selezionato l'approccio basato sulle espressioni regolari come strategia di denominazione delle origini, puoi utilizzare gli esempi di espressioni regolari come guide per le tue espressioni utilizzate nei metodi di risoluzione automatica Data Infrastructure Insights .

Formattazione delle espressioni regolari

Quando si creano espressioni regolari per la risoluzione automatica Data Infrastructure Insights , è possibile configurare il formato di output immettendo valori in un campo denominato *FORMAT*.

L'impostazione predefinita è \1, il che significa che un nome di zona che corrisponde all'espressione regolare viene sostituito dal contenuto della prima variabile creata dall'espressione regolare. In un'espressione regolare, i valori delle variabili vengono creati tramite istruzioni tra parentesi. Se sono presenti più istruzioni tra parentesi, le variabili vengono referenziate numericamente, da sinistra a destra. Le variabili possono essere utilizzate nel formato di output in qualsiasi ordine. È anche possibile inserire del testo costante nell'output, aggiungendolo al campo FORMATO.

Ad esempio, per questa convenzione di denominazione delle zone potrebbero essere disponibili i seguenti nomi di zona:

```
 [Zone number]_[data center]_[hostname]_[device type]_[interface number]
* S123_Miami_hostname1_filer_FC1
* S14_Tampa_hostname2_switch_FC4
* S3991_Boston_hostname3_windows2K_FC0
* S44_Raleigh_hostname4_solaris_FC1
```

E potresti voler ottenere l'output nel seguente formato:

```
 [hostname]-[data center]-[device type]
Per fare ciò, è necessario acquisire i campi nome host, data center e tipo
di dispositivo nelle variabili e utilizzarli nell'output.  La seguente
espressione regolare farebbe questo:
```

```
 .*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
Poiché ci sono tre serie di parentesi, le variabili \1, \2 e \3 verrebbero
popolate.
```

È quindi possibile utilizzare il seguente formato per ricevere l'output nel formato preferito:

```
 \2-\1-\3
Il risultato sarà il seguente:
```

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

I trattini tra le variabili forniscono un esempio di testo costante inserito nell'output formattato.

Esempi

Esempio 1 che mostra i nomi delle zone

In questo esempio, si utilizza l'espressione regolare per estrarre un nome host dal nome della zona. È possibile creare un'espressione regolare se si dispone di qualcosa di simile ai seguenti nomi di zona:

- S0032_myComputer1Name-HBA0
- S0434_nome_mioComputer1-HBA1
- S0432_myComputer1Name-HBA3

L'espressione regolare che potresti utilizzare per catturare il nome host sarebbe:

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
Il risultato è una corrispondenza di tutte le zone che iniziano con S
seguite da una qualsiasi combinazione di cifre, seguite da un trattino
basso, dal nome host alfanumerico (myComputer1Name), da un trattino basso
o un trattino, dalle lettere maiuscole HBA e da una singola cifra (0-9).
Solo il nome host viene memorizzato nella variabile *\1*.
```

L'espressione regolare può essere scomposta nei suoi componenti:

- "S" rappresenta il nome della zona e inizia l'espressione. Corrisponde solo a una "S" all'inizio del nome della zona.
- I caratteri [0-9] tra parentesi indicano che ciò che segue "S" deve essere una cifra compresa tra 0 e 9, inclusi.
- Il segno + indica che l'informazione tra parentesi precedenti deve essere presente 1 o più volte.
- Il carattere _ (trattino basso) indica che le cifre dopo S devono essere seguite immediatamente solo da un carattere di sottolineatura nel nome della zona. In questo esempio, la convenzione di denominazione delle zone utilizza il carattere di sottolineatura per separare il nome della zona dal nome host.
- Dopo il carattere di sottolineatura obbligatorio, le parentesi indicano che il modello contenuto verrà memorizzato nella variabile \1.
- I caratteri tra parentesi quadre [a-zA-Z0-9] indicano che i caratteri corrispondenti sono tutte lettere (indipendentemente dalle maiuscole e dalle minuscole) e numeri.
- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi sono presenti 0 o più volte.
- I caratteri tra parentesi quadre [_-] (trattino basso e trattino) indicano che il modello alfanumerico deve essere seguito da un trattino basso o da un trattino.
- Le lettere HBA nell'espressione regolare indicano che questa esatta sequenza di caratteri deve comparire

nel nome della zona.

- L'ultimo set di caratteri tra parentesi [0-9] corrisponde a una singola cifra da 0 a 9, inclusi.

Esempio 2

In questo esempio, salta fino al primo trattino basso "*", poi abbina E e tutto ciò che segue fino al secondo "*", quindi salta tutto ciò che segue.

Zona: Z_E2FHDBS01_E1NETAPP

Nome host: E2FHDBS01

RegExp: .***?(E.?)***.*?

Esempio 3

Le parentesi "( )" attorno all'ultima sezione nell'espressione regolare (sotto) identificano quale parte è il nome host. Se si desidera che VSAN3 sia il nome host, sarebbe: _([a-zA-Z0-9]).*

Zona: A_VSAN3_SR48KENT_A_CX2578_SPA0

Nome host: SR48KENT

RegExp: _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

Esempio 4 che mostra un modello di denominazione più complicato

È possibile creare un'espressione regolare se si dispone di qualcosa di simile ai seguenti nomi di zona:

- NomeComputer123-HBA1_Symm1_FA3
- NomeComputer123-HBA2_Symm1_FA5
- mioNomeComputer123-HBA3_Symm1_FA7

L'espressione regolare che potresti usare per catturare questi dati sarebbe:

```
 ([a-zA-Z0-9]*)_.*
Dopo essere stata valutata da questa espressione, la variabile \1
conterrebbe solo _myComputerName123_.
```

L'espressione regolare può essere scomposta nei suoi componenti:

- Le parentesi indicano che il modello contenuto verrà memorizzato nella variabile \1.
- I caratteri tra parentesi quadre [a-zA-Z0-9] indicano che qualsiasi lettera (indipendentemente da maiuscole e minuscole) o cifra corrisponderà.
- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi sono presenti 0 o più volte.
- Il carattere _ (trattino basso) nell'espressione regolare indica che il nome della zona deve avere un trattino basso subito dopo la stringa alfanumerica corrispondente alle parentesi quadre precedenti.
- IL . (punto) corrisponde a qualsiasi carattere (carattere jolly).
- Il carattere jolly * (asterisco) indica che il periodo precedente può essere presente 0 o più volte.

In altre parole, la combinazione .* indica qualsiasi carattere, un numero qualsiasi di volte.

Esempio 5 che mostra i nomi delle zone senza un modello

È possibile creare un'espressione regolare se si dispone di qualcosa di simile ai seguenti nomi di zona:

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

L'espressione regolare che potresti usare per catturare questi dati sarebbe:

```
 (.*?)_.*
La variabile \1 conterrebbe _myComputerName_ (nel primo esempio di nome di
zona) o _myComputerName123_ (nel secondo esempio di nome di zona).  Questa
espressione regolare corrisponderebbe quindi a tutto ciò che precede il
primo carattere di sottolineatura.
```

L'espressione regolare può essere scomposta nei suoi componenti:

- Le parentesi indicano che il modello contenuto verrà memorizzato nella variabile \1.
- IL .* (punto e asterisco) corrisponde a qualsiasi carattere, un numero qualsiasi di volte.
- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi sono presenti 0 o più volte.
- Il carattere ? rende la corrispondenza non avida. Ciò costringe il sistema a interrompere la corrispondenza al primo carattere di sottolineatura, anziché all'ultimo.
- I caratteri _.* corrispondono al primo carattere di sottolineatura trovato e a tutti i caratteri che lo seguono.

Esempio 6 che mostra i nomi dei computer con un modello

È possibile creare un'espressione regolare se si dispone di qualcosa di simile ai seguenti nomi di zona:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

L'espressione regolare che potresti usare per catturare questi dati sarebbe:

```
 .*?_.*?_([a-zA-Z0-9]*[ABT])_.*
Poiché la convenzione di denominazione delle zone ha più di uno schema,
potremmo usare l'espressione sopra, che corrisponderà a tutte le istanze
di un nome host (myComputerName nell'esempio) che termina con una A, una B
o una T, inserendo tale nome host nella variabile \1.
```

L'espressione regolare può essere scomposta nei suoi componenti:

- IL .* (punto e asterisco) corrisponde a qualsiasi carattere, un numero qualsiasi di volte.
- Il carattere ? rende la corrispondenza non avida. Ciò costringe il sistema a interrompere la corrispondenza

al primo carattere di sottolineatura, anziché all'ultimo.

- Il carattere di sottolineatura corrisponde al primo carattere di sottolineatura nel nome della zona.
- Pertanto, la prima combinazione .*?_ corrisponde ai caratteri Storage1_ nel primo esempio di nome di zona.
- La seconda combinazione .*?_ si comporta come la prima, ma corrisponde a Switch1_ nel primo esempio di nome di zona.
- Le parentesi indicano che il modello contenuto verrà memorizzato nella variabile \1.
- I caratteri tra parentesi quadre [a-zA-Z0-9] indicano che qualsiasi lettera (indipendentemente da maiuscole e minuscole) o cifra corrisponderà.
- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi sono presenti 0 o più volte.
- I caratteri tra parentesi nell'espressione regolare [ABT] corrispondono a un singolo carattere nel nome della zona che deve essere A, B o T.
- Il carattere _ (trattino basso) che segue le parentesi indica che la corrispondenza del carattere [ABT] deve essere seguita da un trattino basso.
- IL .* (punto e asterisco) corrisponde a qualsiasi carattere, un numero qualsiasi di volte.

Il risultato di ciò farebbe sì che la variabile \1 contenga una qualsiasi stringa alfanumerica che:

- era preceduto da un certo numero di caratteri alfanumerici e due caratteri di sottolineatura
- era seguito da un trattino basso (e poi da un numero qualsiasi di caratteri alfanumerici)
- aveva un carattere finale A, B o T, prima del terzo trattino basso.

Esempio 7

Zona: NomeComputer123_HBA1_Symm1_FA1

Nome host: NomeComputer123

RegExp: ([a-zA-Z0-9]+)_.*

Esempio 8

Questo esempio trova tutto ciò che precede il primo _.

Zona: NomeComputer_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Nome host: NomeComputer

Espressione regolare: (.**?)_.**

Esempio 9

Questo esempio trova tutto ciò che si trova dopo il primo _ e fino al secondo _.

Zona: Z_NomeComputer_NomeArchiviazione

Nome host: Nome del mio computer

RegExp: .***?(.?)***.*?

Esempio 10

Questo esempio estrae "MyComputerName123" dagli esempi di zona.

Zona: Storage1_Switch1_NomeComputer123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

Nome host: NomeComputer123

RegExp: .**?.?**([a-zA-Z0-9]+)**[ABT]_.**

Esempio 11

Zona: Storage1_Switch1_NomeComputer123A_A1_FC1

Nome host: NomeComputer123A

RegExp: .**?.?**([a-zA-z0-9]+).*?

Esempio 12

Il simbolo ^ (accento circonflesso o accento circonflesso) **tra parentesi quadre** nega l'espressione, ad esempio, [^Ff] significa tutto tranne la F maiuscola o minuscola, e [^az] significa tutto tranne le lettere minuscole dalla a alla z, e nel caso precedente, tutto tranne _. L'istruzione format aggiunge "-" al nome host di output.

Zona: mhs_apps44_d_A_10a0_0429

Nome host: mhs-apps44-d

RegExp: ()_([AB]).*Formato in Data Infrastructure Insights: \1-\2 ([^_])_ ()_([^_]).*Formato in Data Infrastructure Insights: \1-\2-\3

Esempio 13

In questo esempio, l'alias di archiviazione è delimitato da "\" e l'espressione deve utilizzare "\\" per definire che nella stringa vengono effettivamente utilizzati dei "\" e che questi non fanno parte dell'espressione stessa.

Alias di archiviazione: \Hosts\E2DOC01C1\E2DOC01N1

Nome host: E2DOC01N1

RegExp: \\.**?\\.**?\\(.*?)

Esempio 14

Questo esempio estrae "PD-RV-W-AD-2" dagli esempi di zona.

Zona: PD_D-PD-RV-W-AD-2_01

Nome host: PD-RV-W-AD-2

RegExp: -(.*-\d).*

Esempio 15

In questo caso l'impostazione del formato aggiunge "US-BV-" al nome host.

Zona: SRV_USBVM11_F1

Nome host: US-BV-M11

RegExp: SRV_USBV([A-Za-z0-9]+)_F[12]

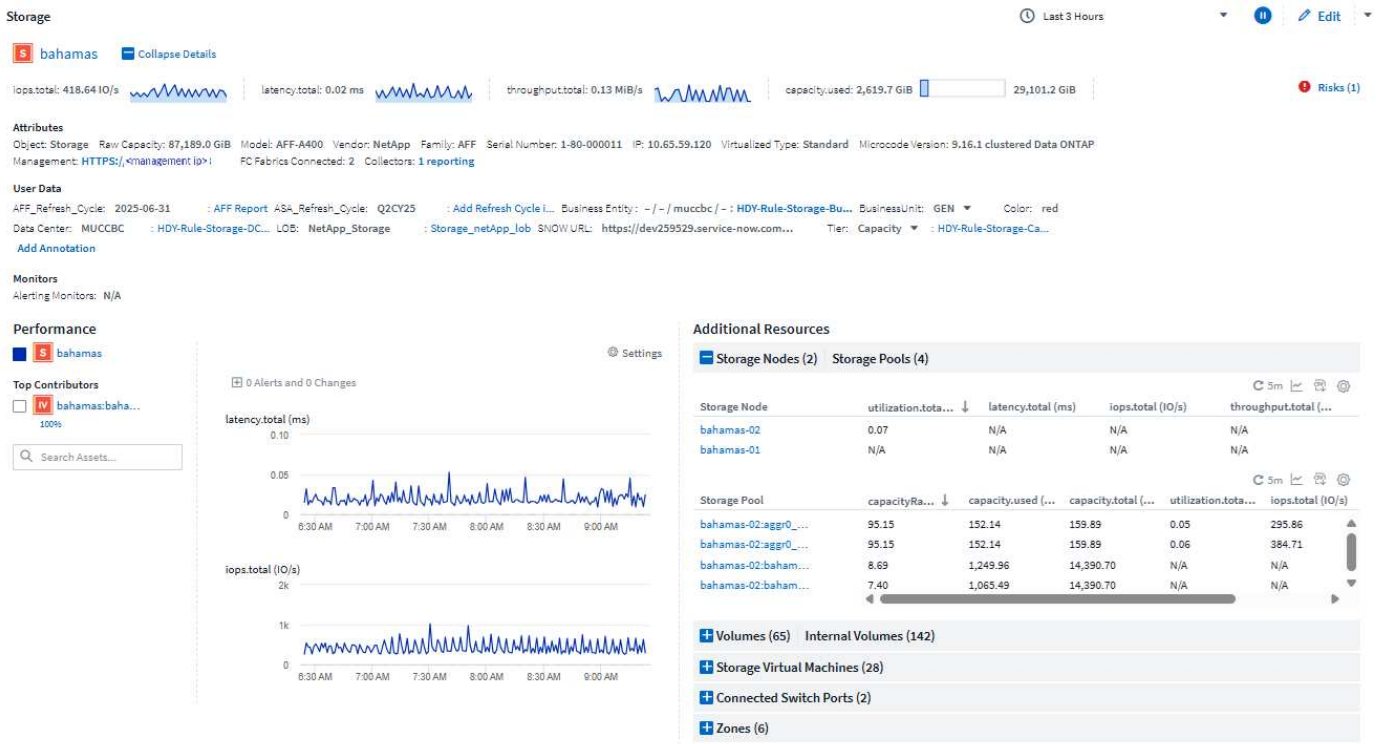
Formato: US-BV-\1

Informazioni sulla pagina delle risorse

Panoramica della pagina delle risorse

Le landing page delle risorse riepilogano lo stato attuale di una risorsa e contengono link a informazioni aggiuntive sulla risorsa e sulle risorse correlate.

Le landing page offrono una visualizzazione dell'oggetto in una sola pagina, con informazioni su Riepilogo, Prestazioni e Risorse correlate.



Sezione Riepilogo

Nella parte superiore di una landing page si trova la sezione espandibile Riepilogo, che include diversi grafici sparkline che mostrano le tendenze recenti dei dati per elementi quali la produttività o la latenza, nonché informazioni e attributi dell'oggetto e qualsiasi monitor che potrebbe emettere avvisi per l'oggetto.

La sezione Riepilogo visualizza e consente anche di modificare le annotazioni assegnate alla risorsa.

Sezione Performance

La sezione Prestazioni visualizza i dati sulle prestazioni dell'oggetto. Selezionare *Impostazioni* per aggiungere grafici aggiuntivi alla visualizzazione, come Throughput o Capacità, oppure selezionare risorse correlate o contribuenti per rappresentare graficamente i loro dati insieme a quelli dell'oggetto. Nella sezione Prestazioni verranno elencati anche i dispositivi che potrebbero potenzialmente causare conflitti. I dati nei grafici vengono aggiornati automaticamente man mano che i raccoglitori di dati interrogano e acquisiscono i dati aggiornati.

Puoi selezionare ilmetrica che si desidera visualizzare nel grafico delle prestazioni per il periodo di tempo selezionato. Fare clic sul menu a discesa *Impostazioni* e scegliere tra le metriche elencate.

Oltre ai dati sulle prestazioni, verranno visualizzati anche tutti gli avvisi attivi o inattivi nell'intervallo di tempo della pagina selezionata.

È possibile selezionare tra i seguenti dispositivi che potrebbero essere elencati nella sezione Prestazioni:

- Principalmente correlato

  Mostra le risorse che presentano un'elevata correlazione (percentuale) con una o più metriche di performance rispetto alla risorsa di base.

- I principali contributori

  Mostra le attività che contribuiscono (in percentuale) all'attività di base.

- Modifiche principali

  Risorse correlate alle modifiche recenti.

- Contese sul carico di lavoro

  Mostra le risorse che hanno un impatto o sono influenzate da altre risorse condivise, come host, reti e storage. A volte vengono chiamate risorse *avide* e *degradate*.

Sezione Risorse aggiuntive

La sezione Risorse aggiuntive visualizza tabelle di dati per le risorse correlate al tipo di oggetto corrente. È possibile espandere e comprimere queste tabelle per concentrarsi su risorse specifiche. Seleziona l'icona dell'ingranaggio per visualizzare temporaneamente metriche o attributi aggiuntivi in una tabella.

Aggiungi widget personalizzati

Puoi aggiungere i tuoi widget a qualsiasi pagina di risorse. I widget aggiunti appariranno nelle pagine delle risorse per tutti gli oggetti di quel tipo. Ad esempio, aggiungendo un widget personalizzato a una pagina di risorse di archiviazione, tale widget verrà visualizzato nelle pagine delle risorse di tutte le risorse di archiviazione.

I widget personalizzati vengono posizionati nella parte inferiore della landing page, sotto le sezioni Prestazioni e Risorse.

Tipi di pagine di risorse

Data Infrastructure Insights fornisce pagine di risorse per le seguenti risorse:

- Macchina virtuale
- Macchina virtuale di archiviazione (SVM)
- Volume
- Volume interno
- Host (incluso Hypervisor)
- Pool di stoccaggio
- Magazzinaggio
- Archivio dati
- Applicazione
- Nodo di archiviazione
- Qtree
- Disco
- VMDK
- Porta
- Interruttore
- Tessuto
- Ospite
- Zona

Modifica dell'intervallo di tempo dei dati visualizzati

Per impostazione predefinita, una pagina di risorse visualizza le ultime 3 ore di dati; tuttavia, è possibile modificare il segmento temporale dei dati visualizzati utilizzando un'opzione presente in ogni pagina di risorse, indipendentemente dal tipo di risorsa. Per modificare l'intervallo di tempo, fare clic sull'intervallo di tempo visualizzato nella barra in alto e scegliere tra i seguenti segmenti di tempo:

- Ultimi 15 minuti

- Ultimi 30 minuti
- Ultimi 60 minuti
- Ultime 2 ore
- Ultime 3 ore (questo è il valore predefinito)
- Ultime 6 ore
- Ultime 12 ore
- Ultime 24 ore
- Ultimi 2 giorni
- Ultimi 3 giorni
- Ultimi 7 giorni
- Ultimi 14 giorni
- Ultimi 30 giorni
- Intervallo di tempo personalizzato

L'intervallo di tempo personalizzato consente di selezionare fino a 31 giorni consecutivi. È anche possibile impostare l'ora di inizio e l'ora di fine del giorno per questo intervallo. L'ora di inizio predefinita è 00:00 del primo giorno selezionato e l'ora di fine predefinita è 23:59 dell'ultimo giorno selezionato. Facendo clic su Applica, l'intervallo di tempo personalizzato verrà applicato alla pagina della risorsa.

Le informazioni sulla pagina si aggiornano automaticamente in base all'intervallo di tempo selezionato. La frequenza di aggiornamento corrente viene visualizzata nell'angolo in alto a destra della sezione Riepilogo e su tutte le tabelle o i widget pertinenti nella pagina.

Definizioni delle metriche di prestazione

La sezione Prestazioni può visualizzare diverse metriche in base al periodo di tempo selezionato per la risorsa. Ogni metrica viene visualizzata nel proprio grafico delle prestazioni. È possibile aggiungere o rimuovere metriche e risorse correlate dai grafici a seconda dei dati che si desidera visualizzare; le metriche tra cui è possibile scegliere variano a seconda del tipo di risorsa.

Metrico	Descrizione
BB credito zero Rx, Tx	Numero di volte in cui il conteggio del credito buffer-to-buffer di ricezione/trasmissione è passato a zero durante il periodo di campionamento. Questa metrica rappresenta il numero di volte in cui la porta collegata ha dovuto interrompere la trasmissione perché non aveva più crediti da fornire.
BB credito durata zero Tx	Tempo in millisecondi durante il quale il credito BB di trasmissione era zero durante l'intervallo di campionamento.
Percentuale di hit della cache (totale, lettura, scrittura) %	Percentuale di richieste che generano hit nella cache. Maggiore è il numero di accessi al volume rispetto agli accessi, migliore è la prestazione. Questa colonna è vuota per gli array di archiviazione che non raccolgono informazioni sui risultati della cache.

Utilizzo della cache (totale) %	Percentuale totale di richieste di cache che danno luogo a hit della cache
Scarti di classe 3	Conteggio degli scarti del trasporto dati Fibre Channel Classe 3.
Utilizzo della CPU (totale) %	Quantità di risorse della CPU utilizzate attivamente, come percentuale del totale disponibile (su tutte le CPU virtuali).
errore CRC	Numero di frame con controlli di ridondanza ciclica (CRC) non validi rilevati dalla porta durante il periodo di campionamento
Frequenza dei fotogrammi	Trasmetti la frequenza dei fotogrammi in fotogrammi al secondo (FPS)
Dimensioni medie del fotogramma (Rx, Tx)	Rapporto tra traffico e dimensione del frame. Questa metrica consente di identificare se nel tessuto sono presenti dei frame sospesi.
Dimensioni del frame troppo lunghe	Conteggio dei frame di trasmissione dati Fibre Channel troppo lunghi.
Dimensioni del telaio troppo corte	Numero di frame di trasmissione dati Fibre Channel troppo brevi.
Densità I/O (totale, lettura, scrittura)	Numero di IOPS diviso per la capacità utilizzata (come acquisita dal sondaggio di inventario più recente dell'origine dati) per l'elemento Volume, Volume interno o Archiviazione. Misurato in numero di operazioni I/O al secondo per TB.
IOPS (totale, lettura, scrittura)	Numero di richieste di servizio I/O di lettura/scrittura che passano attraverso il canale I/O o una parte di tale canale per unità di tempo (misurato in I/O al secondo)
Throughput IP (totale, lettura, scrittura)	Totale: velocità aggregata alla quale i dati IP sono stati trasmessi e ricevuti in megabyte al secondo.
Lettura: Velocità di trasmissione IP (ricezione):	Velocità media di ricezione dei dati IP in megabyte al secondo.
Scrittura: Velocità di trasmissione IP:	Velocità media alla quale venivano trasmessi i dati IP in megabyte al secondo.
Latenza (totale, lettura, scrittura)	Latenza (R&W): velocità con cui i dati vengono letti o scritti sulle macchine virtuali in un intervallo di tempo fisso. Il valore è misurato in megabyte al secondo.
Latenza:	Tempo medio di risposta delle macchine virtuali in un archivio dati.
Latenza massima:	Il tempo di risposta più elevato delle macchine virtuali in un archivio dati.
Errore di collegamento	Numero di guasti di collegamento rilevati dalla porta durante il periodo di campionamento.

Ripristino collegamento Rx, Tx	Numero di ripristini del collegamento di ricezione o trasmissione durante il periodo di campionamento. Questa metrica rappresenta il numero di ripristini di collegamento emessi dalla porta collegata a questa porta.
Utilizzo della memoria (totale) %	Soglia per la memoria utilizzata dall'host.
% R/W parziale (totale)	Numero totale di volte in cui un'operazione di lettura/scrittura attraversa un limite di stripe su qualsiasi modulo disco in un LUN RAID 5, RAID 1/0 o RAID 0. In genere, gli attraversamenti di stripe non sono vantaggiosi, perché ognuno di essi richiede un I/O aggiuntivo. Una percentuale bassa indica una dimensione efficiente dell'elemento stripe ed è indice di un allineamento non corretto di un volume (o di una LUN NetApp). Per CLARiiON, questo valore è il numero di attraversamenti di stripe diviso per il numero totale di IOPS.
Errori di porta	Segnalazione degli errori delle porte durante il periodo di campionamento/intervallo di tempo specificato.
Conteggio delle perdite di segnale	Numero di errori di perdita del segnale. Se si verifica un errore di perdita del segnale, non c'è connessione elettrica e si verifica un problema fisico.
Tasso di swap (tasso totale, tasso di entrata, tasso di uscita)	Velocità con cui la memoria viene trasferita, estratta o entrambe le operazioni dal disco alla memoria attiva durante il periodo di campionamento. Questo contatore si applica alle macchine virtuali.
Conteggio delle perdite di sincronizzazione	Numero di errori di perdita di sincronizzazione. Se si verifica un errore di perdita di sincronizzazione, l'hardware non riesce a dare un senso al traffico o a bloccarlo. È possibile che non tutte le apparecchiature utilizzino la stessa velocità di trasmissione dati oppure che le connessioni ottiche o fisiche siano di scarsa qualità. Dopo ogni errore di questo tipo, la porta deve risincronizzarsi, il che influisce sulle prestazioni del sistema. Misurato in KB/sec.
Throughput (totale, lettura, scrittura)	Velocità con cui i dati vengono trasmessi, ricevuti o entrambi in un intervallo di tempo fisso in risposta alle richieste del servizio I/O (misurata in MB al secondo).
Timeout fotogrammi di scarto - Tx	Conteggio dei frame di trasmissione scartati a causa del timeout.
Velocità di traffico (totale, lettura, scrittura)	Traffico trasmesso, ricevuto o entrambi ricevuti durante il periodo di campionamento, in mebibyte al secondo.
Utilizzo del traffico (totale, lettura, scrittura)	Rapporto tra traffico ricevuto/trasmesso/totale e capacità di ricezione/trasmissione/totale, durante il periodo di campionamento.

Utilizzo (totale, lettura, scrittura) %	Percentuale della larghezza di banda disponibile utilizzata per la trasmissione (Tx) e la ricezione (Rx).
Scrittura in sospeso (totale)	Numero di richieste di servizio di scrittura I/O in sospeso.

Filtraggio per oggetti nel contesto

Quando si configura un widget nella landing page di una risorsa, è possibile impostare filtri *in-context* per mostrare solo gli oggetti direttamente correlati alla risorsa corrente. Per impostazione predefinita, quando aggiungi un widget, vengono visualizzati *tutti* gli oggetti del tipo selezionato nel tuo tenant. I filtri contestuali consentono di visualizzare solo i dati rilevanti per la risorsa corrente.

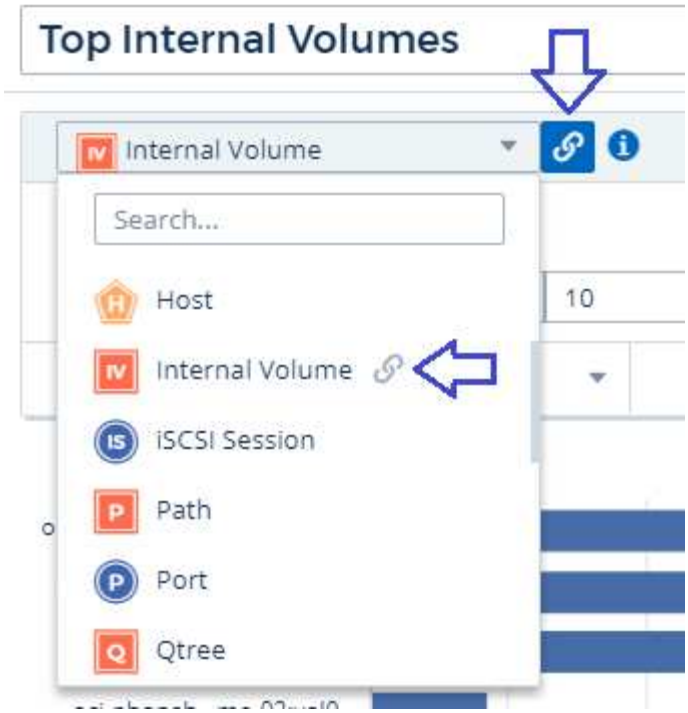
Nella maggior parte delle landing page delle risorse, i widget consentono di filtrare gli oggetti correlati alla risorsa corrente. Nei menu a discesa dei filtri, i tipi di oggetti che visualizzano un'icona di collegamento possono essere filtrati in base al contesto della risorsa corrente.

Ad esempio, in una pagina di risorse di archiviazione, è possibile aggiungere un widget Grafico a barre per visualizzare i valori IOPS più elevati sui volumi interni solo su tale archiviazione. Per impostazione predefinita, quando si aggiunge un widget, vengono visualizzati *tutti* i volumi interni del tenant.

Per visualizzare solo i volumi interni sulla risorsa di archiviazione corrente, procedere come segue:

Passi

1. Apri una pagina delle risorse per qualsiasi risorsa **Archiviazione**.
2. Fare clic su **Modifica** per aprire la pagina delle risorse in modalità di modifica.
3. Fare clic su **Aggiungi widget** e selezionare *Grafico a barre*.
4. Selezionare **Volume interno** come tipo di oggetto da visualizzare nel grafico a barre. Si noti che accanto al tipo di oggetto volume interno è presente un'icona di collegamento. L'icona "collegata" è abilitata per impostazione predefinita.



5. Seleziona *IOPS - Totale* e imposta eventuali filtri aggiuntivi desiderati.
6. Richiudi il campo **Roll Up** cliccando sulla [X] accanto ad esso. Viene visualizzato il campo **Mostra**.
7. Scegli di mostrare i primi 10.
8. Salva il widget.

   Il grafico a barre mostra solo i volumi interni che risiedono sulla risorsa di archiviazione corrente.

Il widget verrà visualizzato nelle pagine delle risorse per tutti gli oggetti di archiviazione. Quando il collegamento contestuale è abilitato nel widget, il grafico a barre mostra i dati per i volumi interni relativi solo alla risorsa di archiviazione attualmente visualizzata.

Per scollegare i dati dell'oggetto, modifica il widget e fai clic sull'icona del collegamento accanto al tipo di oggetto. Il collegamento viene disabilitato e il grafico visualizza i dati per *tutti* gli oggetti nel tenant.

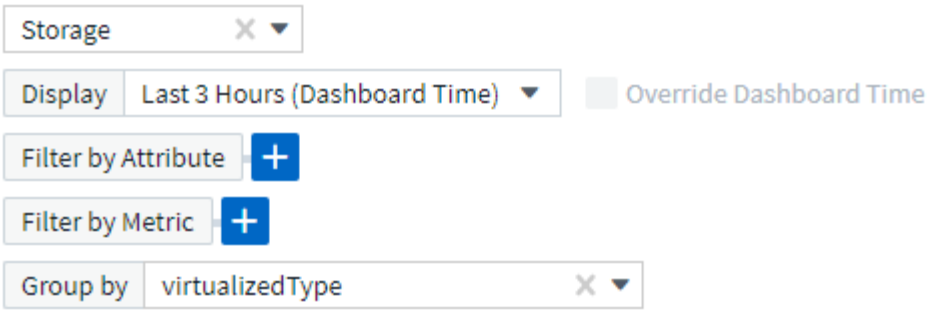
Puoi anche usare**"variabili speciali nei widget"** per visualizzare informazioni relative alle risorse nelle landing page.

Virtualizzazione dello storage

Data Infrastructure Insights è in grado di distinguere tra un array di storage con storage locale e la virtualizzazione di altri array di storage. Ciò ti consente di mettere in relazione i costi e di distinguere le prestazioni dal front-end fino al back-end della tua infrastruttura.

Virtualizzazione in un widget di tabella

Uno dei modi più semplici per iniziare a esaminare la virtualizzazione dello storage è creare un widget tabella dashboard che mostri il tipo Virtualizzato. Quando si crea la query per il widget, è sufficiente aggiungere "virtualizedType" al raggruppamento o al filtro.



Il widget della tabella risultante mostra gli archivi *Standard*, *Backend* e *Virtual* sul tuo tenant.

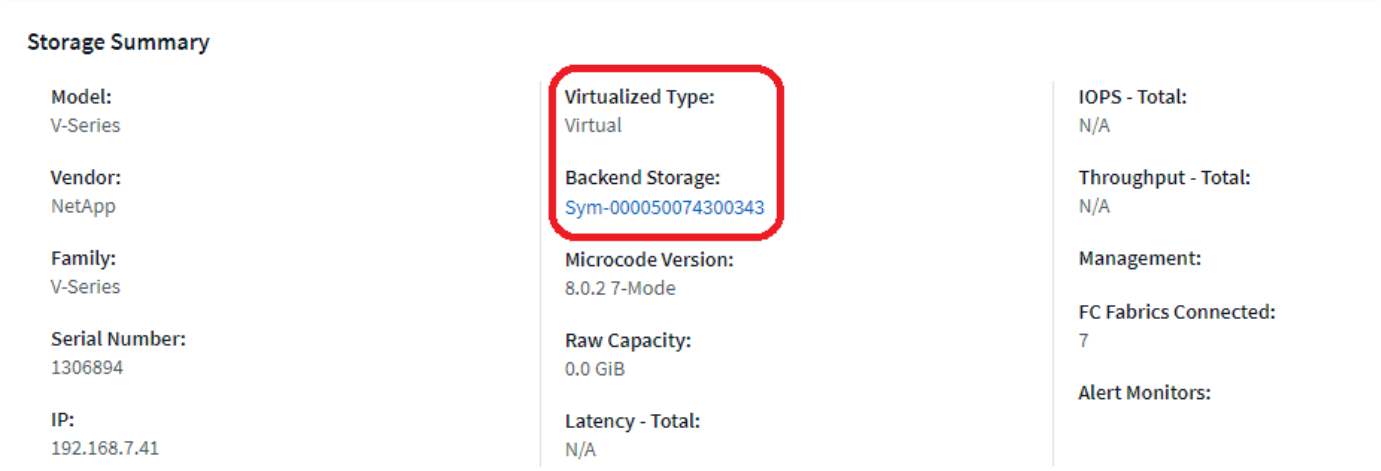
Storage by virtualizedType

50 items found in 4 groups

virtualizedType	Storage
Backend (5)	--
Backend	Sym-Perf
Backend	Sym-000050074300343
Backend	CX600_26_CK00351029326
Backend	VNX8000_46_CK00351029346
Backend	Sym-000050074300324
Standard (36)	--
Virtual (8)	--

Le landing page mostrano informazioni virtualizzate

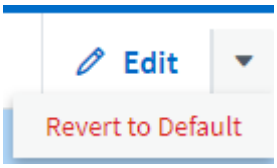
Nella landing page di un archivio, di un volume, di un volume interno o di un disco, puoi visualizzare le informazioni rilevanti sulla virtualizzazione. Ad esempio, osservando la landing page di storage qui sotto, puoi vedere che si tratta di un storage virtuale e a quale sistema di storage back-end si applica. Tutte le tabelle pertinenti nelle landing page mostreranno anche le informazioni sulla virtualizzazione, se applicabili.



Pagine di destinazione e dashboard esistenti

Tieni presente che se attualmente disponi di landing page o dashboard personalizzate sul tuo tenant, queste non mostreranno automaticamente tutte le informazioni sulla virtualizzazione per impostazione predefinita. Tuttavia, è possibile *ripristinare le impostazioni predefinite* di qualsiasi dashboard o landing page personalizzata (sarà necessario reimplementare le personalizzazioni) oppure modificare i widget pertinenti per includere gli attributi o le metriche di virtualizzazione desiderati.

Ripristina impostazioni predefinite è disponibile nell'angolo in alto a destra di una dashboard personalizzata o di una schermata di landing page.



Suggerimenti e consigli per cercare risorse e avvisi

Per ricercare dati o oggetti nell'ambiente monitorato è possibile utilizzare diverse tecniche di ricerca.

- **Ricerca con caratteri jolly**

  È possibile eseguire una ricerca con più caratteri jolly utilizzando il carattere *. Ad esempio, *applic*n* restituirebbe *application*.

- **Frasi utilizzate nella ricerca**

  Una frase è un gruppo di parole racchiuso tra virgolette doppie, ad esempio "VNX LUN 5". È possibile utilizzare le virgolette doppie per cercare documenti che contengono spazi nei loro nomi o attributi.

- **Operatori booleani**

  Utilizzando gli operatori booleani OR, AND e NOT, è possibile combinare più termini per formare una query più complessa.

  O

L’operatore OR è l’operatore di congiunzione predefinito.

Se non esiste alcun operatore booleano tra due termini, viene utilizzato l’operatore OR.

L’operatore OR collega due termini e trova un documento corrispondente se uno dei due termini è presente in un documento.

Ad esempio, *storage OR netapp* cerca i documenti che contengono *storage* o *netapp*.

I punteggi più alti vengono assegnati ai documenti che corrispondono alla maggior parte dei termini.

E

È possibile utilizzare l’operatore AND per trovare documenti in cui entrambi i termini di ricerca sono presenti in un unico documento. Ad esempio, *storage AND netapp* cerca i documenti che contengono sia *storage* che *netapp*.

È possibile utilizzare il simbolo **&&** al posto della parola AND.

NON

Quando si utilizza l’operatore NOT, tutti i documenti che contengono il termine dopo NOT vengono esclusi dai risultati della ricerca. Ad esempio, *storage NOT netapp* cerca i documenti che contengono solo *storage* e non *netapp*.

È possibile utilizzare il simbolo **!** al posto della parola NOT.

La ricerca non distingue tra maiuscole e minuscole.

Ricerca tramite termini indicizzati

Le ricerche che corrispondono a un numero maggiore di termini indicizzati generano punteggi più alti.

La stringa di ricerca viene suddivisa in termini di ricerca separati tramite uno spazio. Ad esempio, la stringa di ricerca "storage aurora netapp" è suddivisa in tre parole chiave: "storage", "aurora" e "netapp". La ricerca viene effettuata utilizzando tutti e tre i termini. I documenti che corrispondono alla maggior parte di questi termini avranno il punteggio più alto. Più informazioni fornisci, migliori saranno i risultati della ricerca. Ad esempio, è possibile cercare un archivio in base al nome e al modello.

L’interfaccia utente visualizza i risultati della ricerca per categorie, con i tre risultati principali per categoria. Se non hai trovato l’oggetto che ti aspettavi, puoi includere più termini nella stringa di ricerca per migliorare i risultati della ricerca.

La tabella seguente fornisce un elenco di termini indicizzati che possono essere aggiunti alla stringa di ricerca.

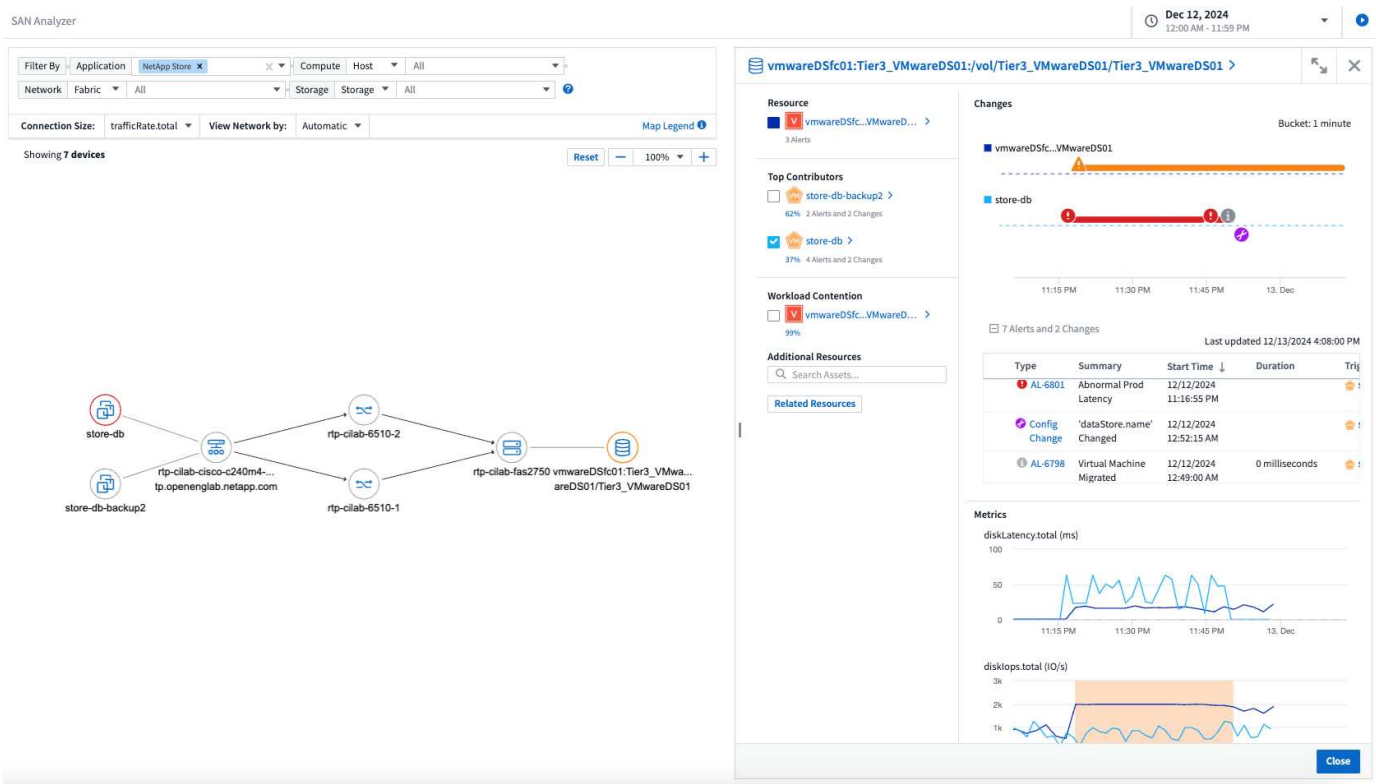
Categoria	Termini indicizzati
Magazzinaggio	modello del fornitore del nome "storage"
StoragePool	"storagepool" nome nome dell’archiviazione indirizzi IP dell’archiviazione numero di serie dell’archiviazione fornitore dell’archiviazione modello di archiviazione nomi per tutti i volumi interni associati nomi per tutti i dischi associati

Categoria	Termini indicizzati
Volume interno	"internalvolume" nome nome dell'archiviazione indirizzi IP dell'archiviazione numero di serie dell'archiviazione fornitore dell'archiviazione modello di archiviazione nome del pool di archiviazione nomi di tutte le condivisioni associate nomi di tutte le applicazioni associate
Volume	etichetta del nome "volume" nomi di tutti i volumi interni nome del pool di archiviazione nome dell'archiviazione indirizzi IP dell'archiviazione numero di serie dell'archiviazione fornitore dell'archiviazione modello di archiviazione
Nodo di archiviazione	"storagenode" nome nome dell'archiviazione indirizzi IP dell'archiviazione numero di serie dell'archiviazione fornitore dell'archiviazione modello di archiviazione
Ospite	nome "host" indirizzi IP nomi di tutte le applicazioni associate
Archivio dati	nome "datastore" centro virtuale nomi IP di tutti i volumi nomi di tutti i volumi interni
Macchine virtuali	nome "virtualmachine" nome DNS indirizzi IP nome dell'host indirizzi IP dell'host nomi di tutti i datastore nomi di tutte le applicazioni associate
Interruttori (normali e NPV)	"switch" indirizzo IP nome wwn numero di serie modello ID dominio nome del fabric wwn del fabric
Applicazione	nome "applicazione" tenant linea di business unità aziendale progetto
Nastro	"nastro" indirizzo IP nome numero di serie fornitore
Porta	nome wwn "porta"
Tessuto	nome wwn "fabric"
Macchina virtuale di archiviazione (SVM)	UUID del nome "storagevirtualmachine"

Analisi dei dati

Panoramica dell'analizzatore SAN

La SAN svolge un ruolo cruciale nella gestione di carichi di lavoro vitali, ma la sua complessità può causare interruzioni significative e disagi per i clienti. Con **SAN Analyzer** di DII, la gestione della SAN diventa più semplice ed efficiente. Questo potente strumento offre visibilità end-to-end, mappando le dipendenze da VM/host a rete, LUN e storage. Grazie a una mappa topologica interattiva, SAN Analyzer consente di individuare i problemi, comprendere i cambiamenti e migliorare la comprensione del flusso di dati. Semplifica la gestione SAN in ambienti IT complessi con SAN Analyzer e aumenta la visibilità sui carichi di lavoro a blocchi.



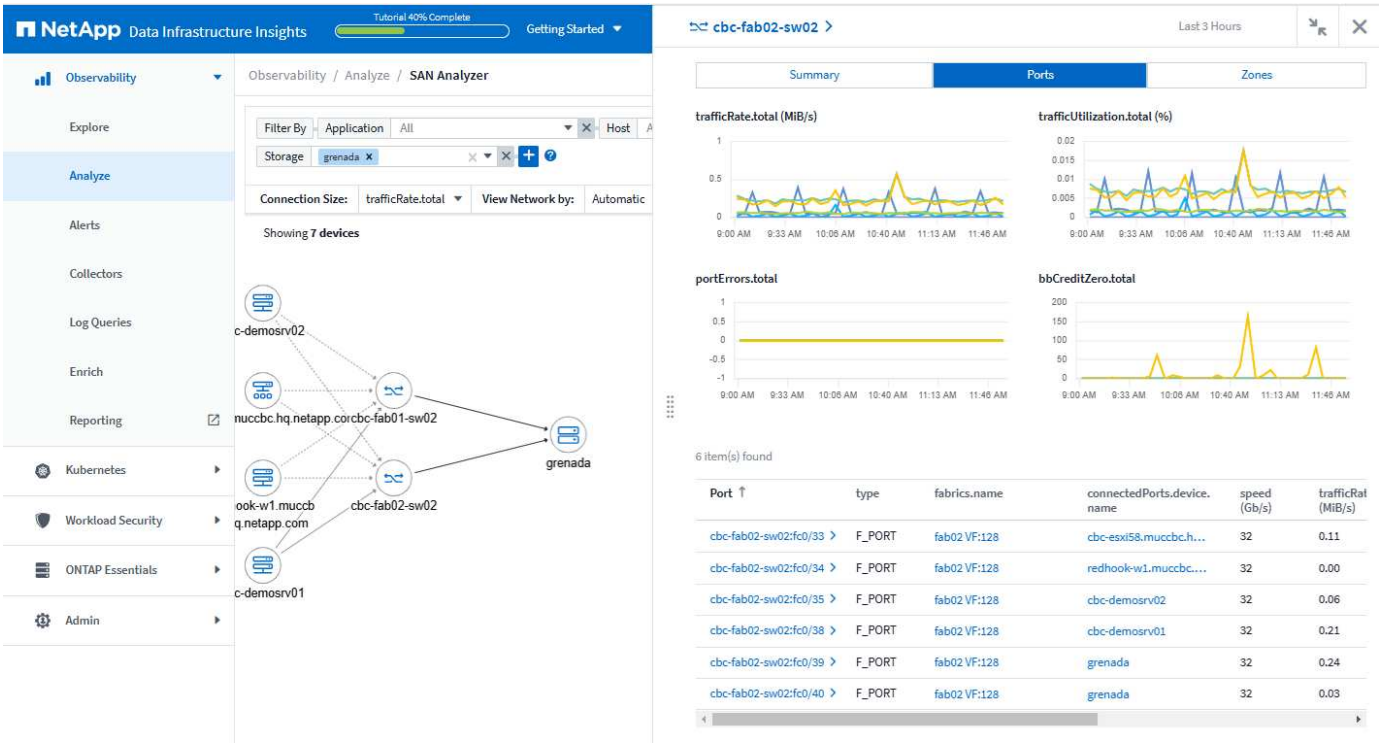
Esplora le connessioni tra le tue risorse

Selezionare **Osservabilità > Analizza > Analizzatore SAN** per visualizzare l'analizzatore SAN. Imposta un filtro per Applicazione, Host, Fabric e/o Storage. Viene visualizzata la mappa degli oggetti, che mostra gli oggetti collegati. Passa il mouse su un oggetto per visualizzare le metriche del traffico per quelle connessioni.

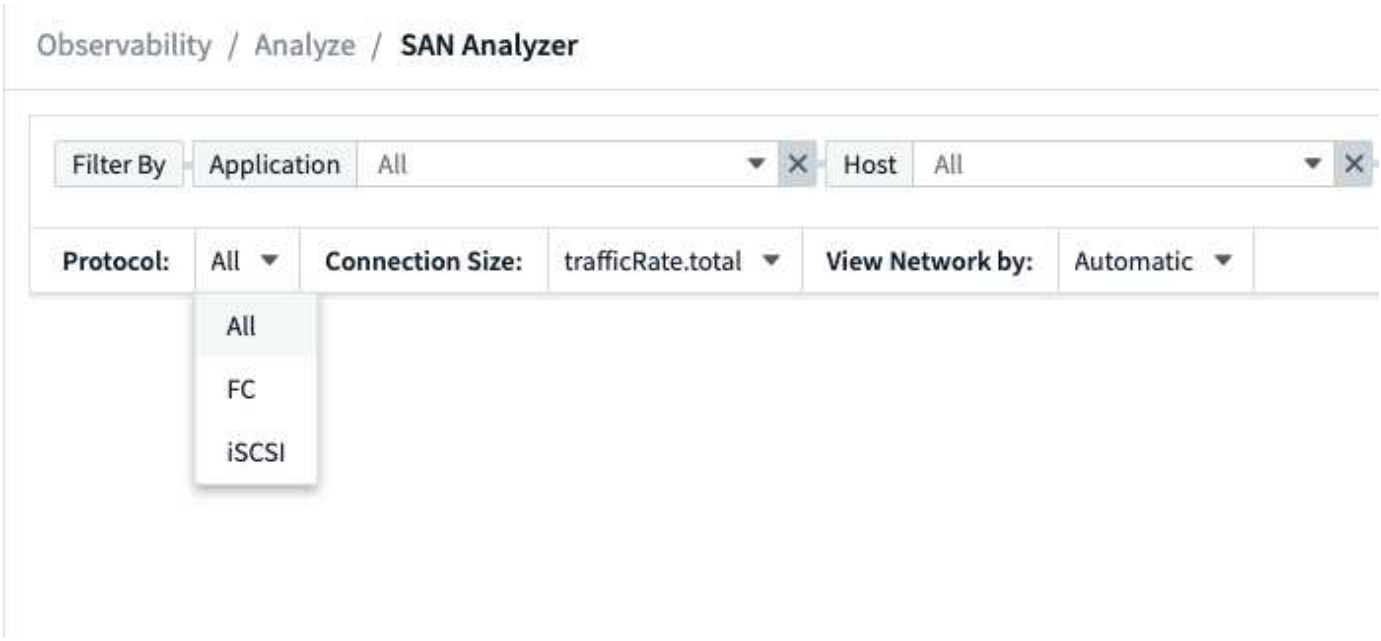
La maggior parte dei filtri di SAN Analyzer (inclusi quelli che puoi aggiungere) sono contestuali; quando selezioni un oggetto in uno di questi filtri, le scelte presentate negli altri menu a discesa dei filtri vengono aggiornate in base al contesto dell'oggetto o degli oggetti selezionati. Le uniche eccezioni sono Applicazione, Porta e Switch; questi filtri non sono contestuali.

Facendo clic su un oggetto o un gruppo si apre un pannello scorrevole che fornisce ulteriori dettagli sull'oggetto e sulle sue connessioni. Il pannello scorrevole visualizza un riepilogo che fornisce dettagli sull'oggetto selezionato (ad esempio, IP, Hypervisor, Connected Fabric, ecc., a seconda del tipo di oggetto) e grafici che mostrano le metriche per l'oggetto, come latenza o IOPS, nonché modifiche e avvisi, se pertinenti. Se lo desideri, puoi anche scegliere di visualizzare le metriche per gli oggetti più correlati nei grafici.

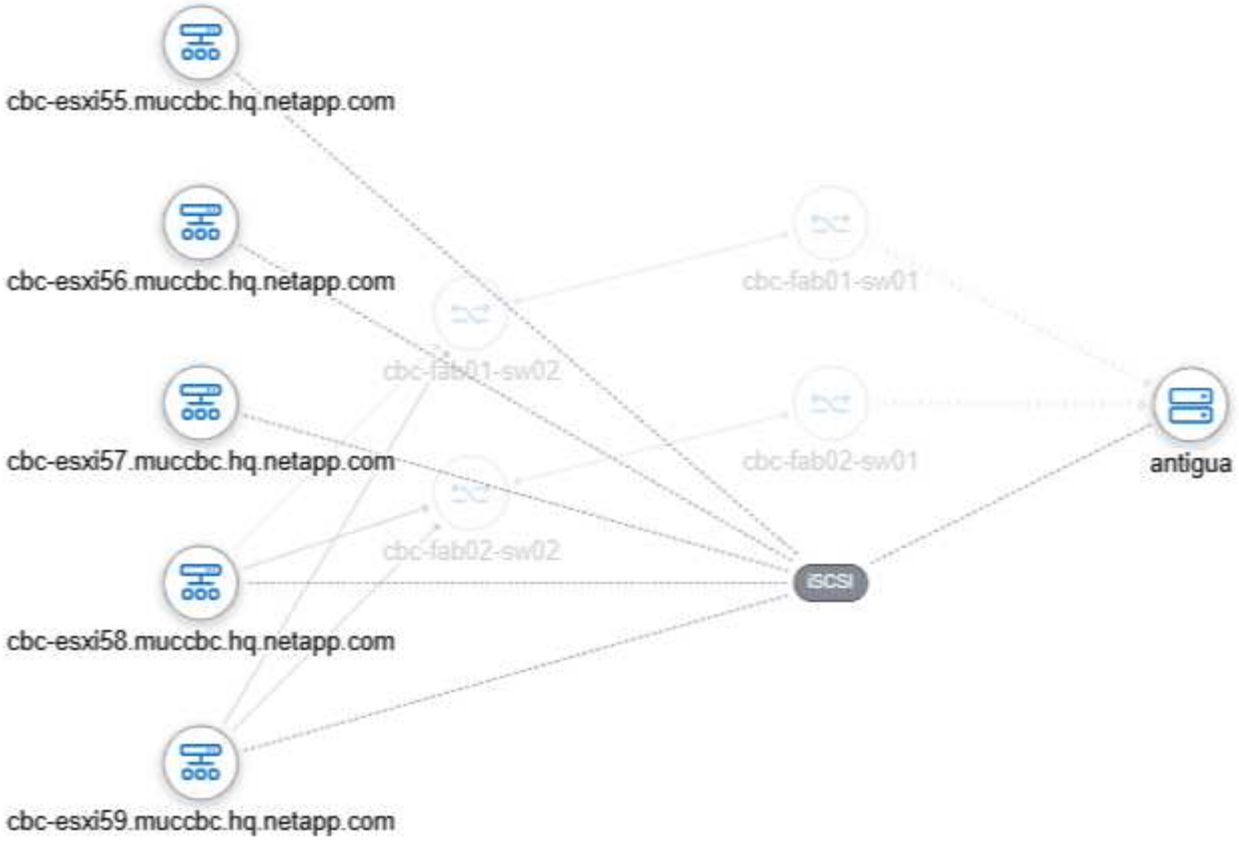
Oltre alla scheda Riepilogo, il pannello scorrevole visualizza schede per informazioni quali i dettagli della porta o le informazioni sulla zona, a seconda dell'oggetto scelto.



Se il tuo ambiente ha protocolli diversi, puoi filtrare per iSCSI o FC:



Se l'ambiente include dispositivi iSCSI, passando il mouse sull'oggetto *iSCSI* vengono evidenziate le connessioni relative a tali dispositivi iSCSI.



Suggerimenti per la risoluzione dei problemi

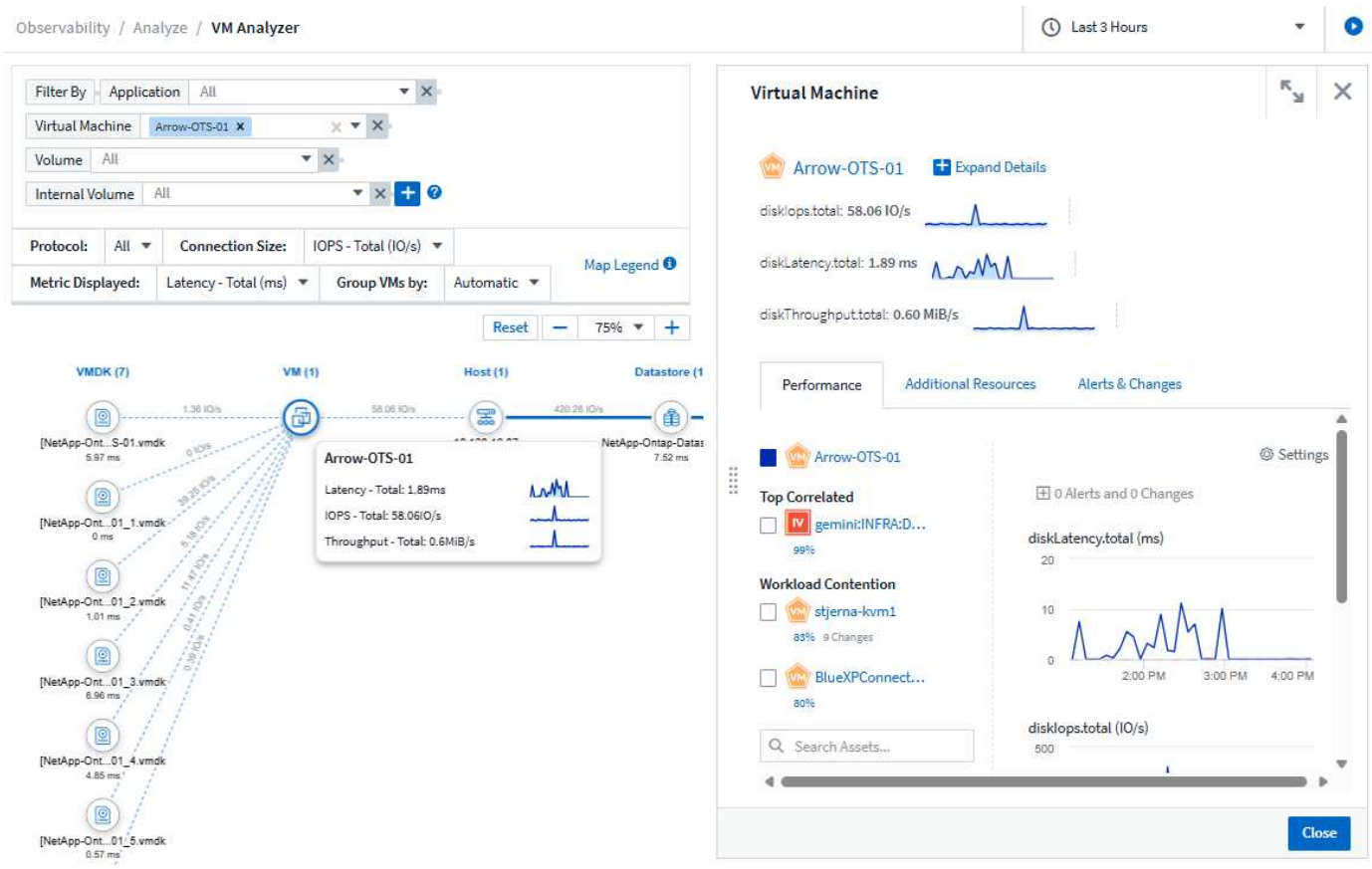
Ecco alcune cose da provare se riscontri problemi:

Problema:	Prova questo:
Vedo <0, =0 o >0 nella legenda per metriche come *trafficUtilization* o *trafficRate*.	Ciò potrebbe verificarsi in casi molto rari in cui i valori metrici sono inferiori a due cifre decimali, ad esempio 0,000123. Ampliare la finestra temporale potrebbe aiutare ad analizzare la metrica in modo più efficace.

Panoramica di VM Analyzer

Con **VM Analyzer** di DII, la gestione delle risorse virtuali diventa più semplice ed efficiente. Questo potente strumento offre visibilità end-to-end, mappando le dipendenze da VMDK/VM a Host, a Datastore, a Volume interno/Volume a Storage.

Grazie a una mappa topologica interattiva, VM Analyzer consente di individuare i problemi, comprendere i cambiamenti e migliorare la comprensione del flusso di dati. Semplifica la gestione delle VM e aumenta la visibilità sui carichi di lavoro virtuali.



Esplora le connessioni tra le tue risorse

Selezionare **Osservabilità > Analizza > Analizzatore VM** per visualizzare l'analizzatore VM. Imposta un filtro per Applicazione, Macchina virtuale, Volume, Volume interno oppure aggiungi i tuoi filtri. Viene visualizzata la mappa degli oggetti, che mostra gli oggetti collegati. Passa il mouse su un oggetto per visualizzare le metriche del traffico per quelle connessioni.

La maggior parte dei filtri di VM Analyzer (inclusi quelli che puoi aggiungere) sono contestuali; quando selezioni un oggetto in uno di questi filtri, le scelte presentate negli altri menu a discesa dei filtri vengono aggiornate in base al contesto dell'oggetto o degli oggetti selezionati.

Facendo clic su un oggetto o un gruppo si apre un pannello scorrevole che fornisce ulteriori dettagli sull'oggetto e sulle sue connessioni. Il pannello scorrevole visualizza un riepilogo che fornisce dettagli sull'oggetto selezionato (ad esempio, produttività o utilizzo, a seconda del tipo di oggetto) e grafici che mostrano le metriche per l'oggetto, come latenza o IOPS. Le schede aggiuntive consentono di esplorare risorse aggiuntive correlate o modifiche e avvisi. Se lo si desidera, è possibile scegliere di visualizzare anche

le metriche per gli oggetti più correlati o in competizione nei grafici.

Guardalo in azione

Risoluzione dei problemi semplificata con VM Analyzer (video),window=read-later

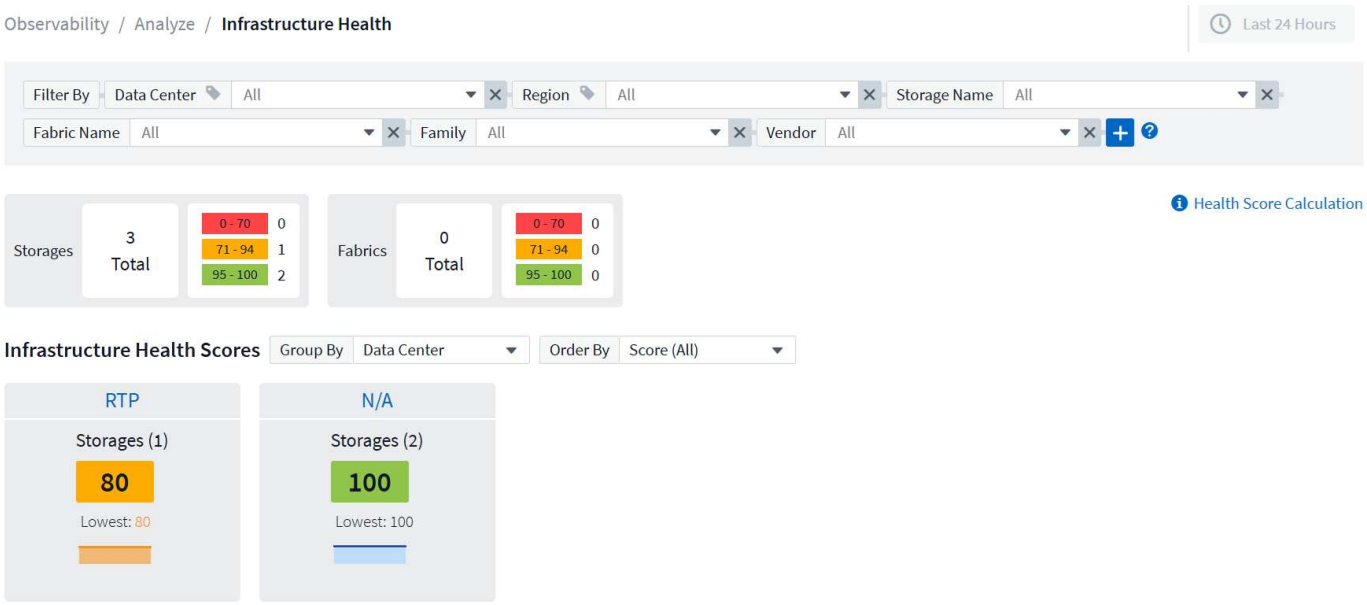
Monitorare lo stato di salute delle infrastrutture

Data Infrastructure Insights fornisce un monitoraggio completo dello stato dell'infrastruttura che tiene traccia delle prestazioni, della capacità, della configurazione e dello stato dei componenti del tuo ambiente di archiviazione. I punteggi di integrità vengono calcolati in base agli avvisi di monitoraggio in queste categorie, offrendo una visione unificata dello stato di integrità del sistema e consentendo una risoluzione proattiva dei problemi.

Il dashboard sulla salute delle infrastrutture

> Il monitoraggio della salute delle infrastrutture è un"Anteprima" funzionalità ed è soggetta a modifiche.

Vai su **Osservabilità > Analizza** e seleziona **Stato dell'infrastruttura**. La dashboard fornisce una panoramica dello stato di salute del sistema, in base alle categorie di avviso del monitor e ai punteggi, come spiegato di seguito. Imposta i filtri in alto per restringere il campo della tua indagine.



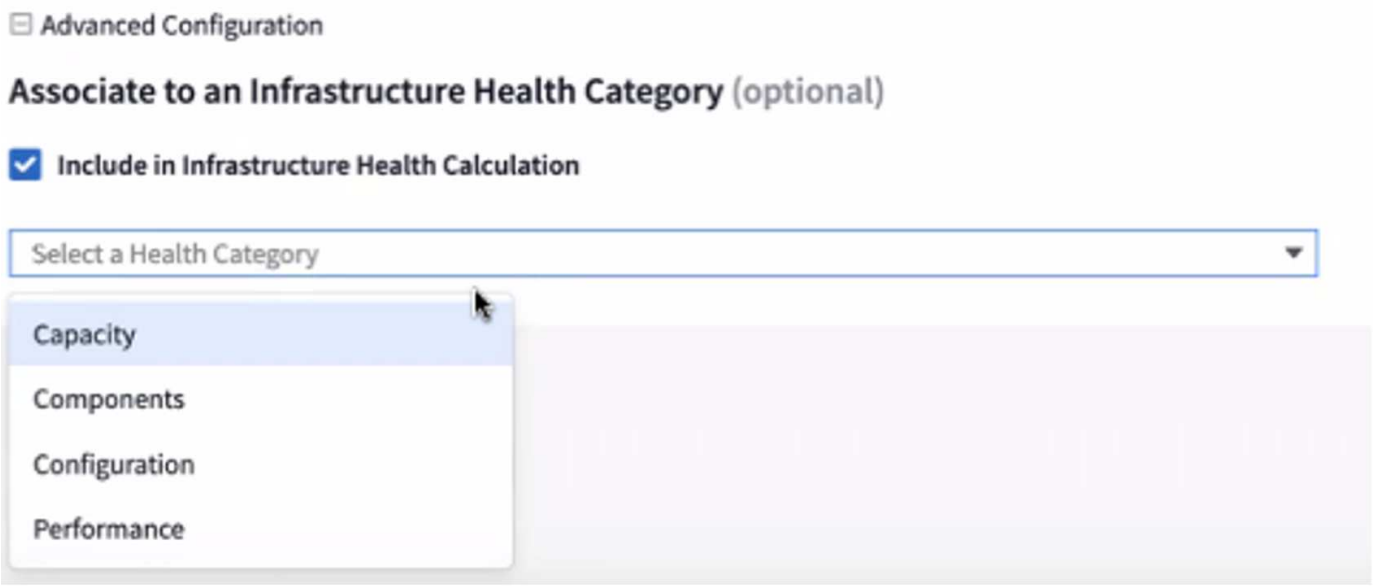
Per impostazione predefinita, i punteggi di integrità sono raggruppati per data center; puoi selezionare il raggruppamento più adatto alla tua sessione.

Configurare i monitor da utilizzare per lo stato dell'infrastruttura

I punteggi di integrità sono determinati da avvisi configurati per l'inclusione nei calcoli di integrità del sistema.

Quando si crea un monitor per un oggetto infrastrutturale, è possibile scegliere se includere gli avvisi del monitor nei calcoli. Nella parte inferiore dello schermo, espandi Configurazione avanzata e seleziona *Includi nel calcolo dello stato dell'infrastruttura*. Selezionare una categoria a cui applicare il calcolo per il monitor:

- **Stato dei componenti**: guasto della ventola, processore di servizio offline, ecc.
- **Stato delle prestazioni**: elevato utilizzo dei nodi di archiviazione, picco anomalo nella latenza dei nodi, ecc.
- **Stato della capacità**: capacità del pool di archiviazione quasi piena, spazio insufficiente per snapshot LUN, ecc.
- **Stato della configurazione**: livello cloud non raggiungibile, relazione SnapMirror non sincronizzata, ecc.



Spiegazione dei punteggi di salute

I punteggi vengono presentati su una scala da 0 a 100, dove 100 corrisponde a piena salute. Gli oggetti infrastrutturali monitorati che presentano problemi attuali o recenti abbasseranno questo punteggio in base alle seguenti medie ponderate:

- Componenti, prestazioni o capacità: 30% ciascuno
- Configurazione: 10%

I punteggi di integrità sono influenzati dagli avvisi generati dai monitor configurati per essere inclusi nei calcoli di integrità dell'infrastruttura nei seguenti modi:

- Gli avvisi critici abbassano il punteggio di salute del peso della categoria *completa*
- Gli avvisi di avvertimento abbassano il punteggio di *metà* del peso della categoria.

Se una categoria non viene segnalata, la media ponderata verrà adeguata di conseguenza.

Ad esempio: 1 avviso critico sui Componenti (-30) e 1 avviso di avvertenza sulle Prestazioni (50% di 30 = -15) producono un punteggio di integrità di 55 (100 meno 45).

Una volta risolti gli avvisi, le riduzioni del punteggio di integrità diminuiscono gradualmente e il punteggio viene ripristinato completamente entro 2 ore.

Segnalazione

Panoramica dei report di Data Infrastructure Insights Insights

Il reporting di Data Infrastructure Insights è uno strumento di business intelligence che consente di visualizzare report predefiniti o di creare report personalizzati.

La funzionalità di reporting è disponibile in Data Infrastructure Insights"Edizione Premium" . La disponibilità della funzionalità di reporting è soggetta a un requisito di ingombro minimo. "Contatta il tuo rappresentante commerciale NetApp" per maggiori informazioni.

Con i report di Data Infrastructure Insights puoi svolgere le seguenti attività:

- Esegui un report predefinito
- Crea un report personalizzato
- Personalizza il formato e il metodo di consegna di un report
- Pianifica l'esecuzione automatica dei report
- Rapporti via e-mail
- Utilizzare i colori per rappresentare le soglie sui dati

Data Infrastructure Insights Reporting può generare report personalizzati per aree quali chargeback, analisi dei consumi e previsioni e può aiutare a rispondere a domande come le seguenti:

- Che inventario ho?
- Dov'è il mio inventario?
- Chi utilizza i nostri beni?
- A cosa si riferisce il chargeback per lo spazio di archiviazione assegnato a un'unità aziendale?
- Quanto tempo ci vorrà prima che io abbia bisogno di acquisire ulteriore capacità di archiviazione?
- Le unità aziendali sono allineate lungo i livelli di archiviazione appropriati?
- Come cambia l'allocazione dello spazio di archiviazione nel corso di un mese, un trimestre o un anno?

Accesso ai report Data Infrastructure Insights

È possibile accedere a Data Infrastructure Insights Reporting facendo clic sul collegamento **Report** nel menu.

Verrai indirizzato all'interfaccia di reporting. Data Infrastructure Insights utilizza IBM Cognos Analytics per il suo motore di reporting.

Che cos'è ETL?

Quando si lavora con la creazione di report, si sentiranno i termini "Data Warehouse" ed "ETL". ETL è l'acronimo di "Extract, Transform, and Load". Il processo ETL recupera i dati raccolti in Data Infrastructure Insights e li trasforma in un formato utilizzabile nella creazione di report. Per "Data Warehouse" si intendono i dati raccolti disponibili per la creazione di report.

Il processo ETL comprende i seguenti processi individuali:

- **Estratto**: estrae i dati da Data Infrastructure Insights.
- **Trasforma**: applica regole o funzioni logiche aziendali ai dati così come vengono estratti da Data Infrastructure Insights.

- **Carica**: salva i dati trasformati nel data warehouse per utilizzarli nella creazione di report.

Ruoli utente dei report di Data Infrastructure Insights

Se disponi di Data Infrastructure Insights Premium Edition con Reporting, ogni utente Data Infrastructure Insights nel tuo tenant avrà anche un accesso Single Sign-On (SSO) all'applicazione Reporting (ad esempio Cognos). Basta cliccare sul link **Report** nel menu e si accederà automaticamente alla sezione Report.

Il tuo ruolo utente in Data Infrastructure Insights determina il tuo ruolo utente di Reporting:

Ruolo Data Infrastructure Insights	Ruolo di segnalazione	Autorizzazioni di segnalazione
Ospite	Consumatore	È possibile visualizzare, pianificare ed eseguire report e impostare preferenze personali, come quelle relative a lingue e fusi orari. I consumatori non possono creare report o svolgere attività amministrative.
Utente	Autore	Può eseguire tutte le funzioni del consumatore, nonché creare e gestire report e dashboard.
Amministratore	Amministratore	Può eseguire tutte le funzioni dell'autore nonché tutte le attività amministrative, come la configurazione dei report e l'arresto e il riavvio delle attività di reporting.

Nella tabella seguente sono illustrate le funzioni disponibili per ciascun ruolo di reporting.

Caratteristica	Consumatore	Autore	Amministratore
Visualizza i report nella scheda Contenuto del team	SÌ	SÌ	SÌ
Esegui report	SÌ	SÌ	SÌ
Pianifica i report	SÌ	SÌ	SÌ
Carica file esterni	NO	SÌ	SÌ
Crea posti di lavoro	NO	SÌ	SÌ
Crea storie	NO	SÌ	SÌ
Crea report	NO	SÌ	SÌ
Crea pacchetti e moduli dati	NO	SÌ	SÌ
Svolgere compiti amministrativi	NO	NO	SÌ

Aggiungi/modifica elemento HTML	NO	NO	SÌ
Esegui report con elemento HTML	SÌ	SÌ	SÌ
Aggiungi/modifica SQL personalizzato	NO	NO	SÌ
Esegui report con SQL personalizzato	SÌ	SÌ	SÌ

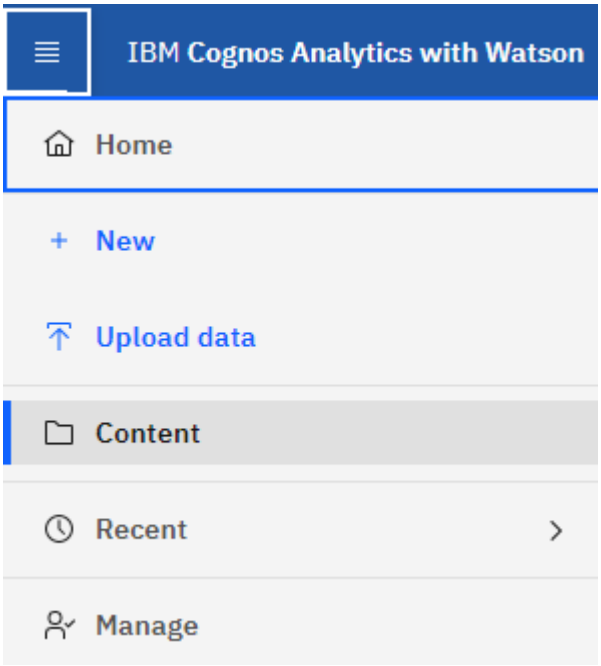
Impostazione delle preferenze e-mail di Reporting (Cognos)

Se modifichi le preferenze e-mail dell'utente in Data Infrastructure Insights Reporting (ovvero l'applicazione Cognos), tali preferenze saranno attive *solo per la sessione corrente*. Uscendo da Cognos e riaccedendo, le tue preferenze e-mail verranno reimpostate.

Quali passaggi dovrei seguire per preparare il mio ambiente esistente all'abilitazione dell'SSO?

Per garantire che i tuoi report vengano conservati, migra tutti i report da *I miei contenuti* a *Contenuti del team* seguendo i passaggi seguenti. Devi fare questo prima di abilitare SSO sul tuo tenant:

1. Vai a **Menu > Contenuto**



1. Crea una nuova cartella in ***Team Content***
   a. Se sono stati creati più utenti, creare una cartella separata per ogni utente per evitare di sovrascrivere i report con nomi duplicati
2. Vai a *I miei contenuti*
3. Seleziona tutti i report che desideri conservare.
4. Nell'angolo in alto a destra del menu, seleziona "Copia o sposta"
5. Passare alla cartella appena creata in *Team Content*

6. Incolla i report nella cartella appena creata utilizzando i pulsanti "Copia in" o "Sposta in"
7. Una volta abilitato l'SSO per Cognos, accedi a Data Infrastructure Insights con l'indirizzo email utilizzato per creare il tuo account.
8. Passare alla cartella *Team Content* in Cognos e copiare o spostare i report salvati in precedenza in *My Content*.

Report predefiniti semplificati

Data Infrastructure Insights Reporting include report predefiniti che soddisfano una serie di requisiti di reporting comuni, fornendo informazioni critiche di cui le parti interessate hanno bisogno per prendere decisioni informate sulla propria infrastruttura di storage.

La funzionalità di reporting è disponibile in Data Infrastructure Insights"Edizione Premium" .

È possibile generare report predefiniti dal Data Infrastructure Insights Reporting Portal, inviarli tramite e-mail ad altri utenti e persino modificarli. Diversi report consentono di filtrare per dispositivo, entità aziendale o livello. Gli strumenti di reporting utilizzano IBM Cognos come base e offrono numerose opzioni di presentazione dei dati.

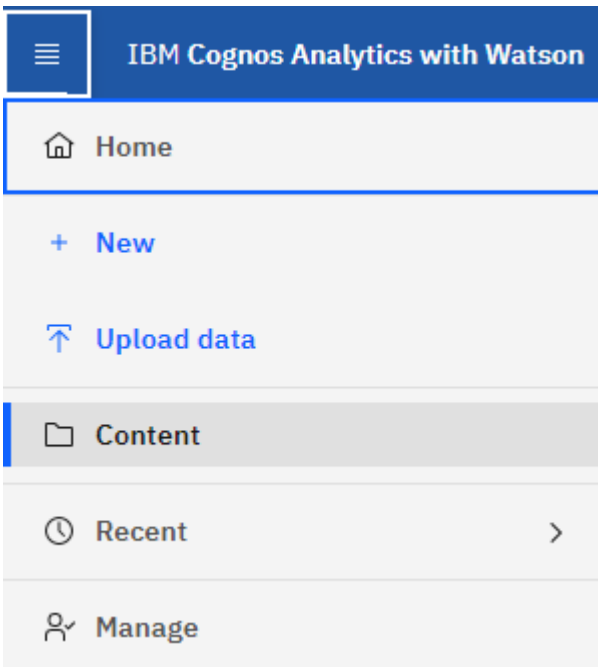
I report predefiniti mostrano i dati relativi a inventario, capacità di archiviazione, addebiti, prestazioni, efficienza di archiviazione e costi del cloud. È possibile modificare questi report predefiniti e salvare le modifiche.

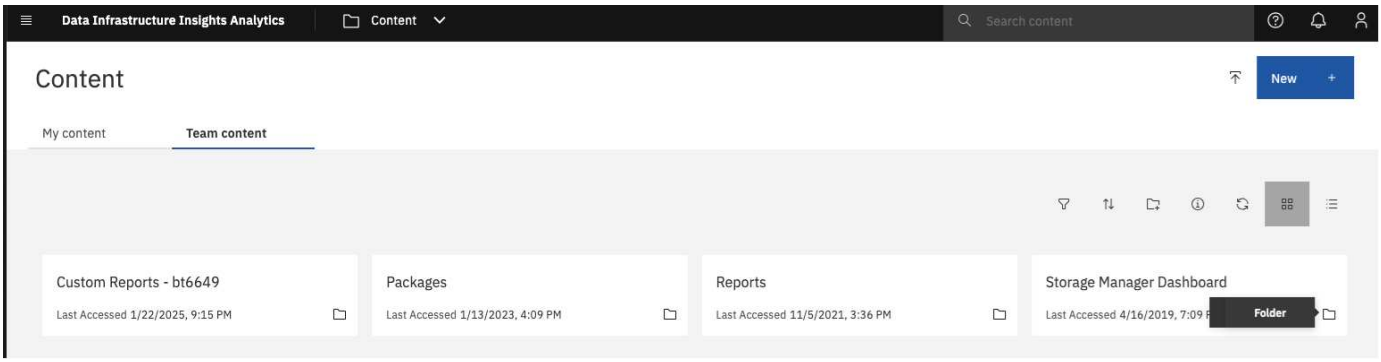
È possibile generare report in vari formati, tra cui HTML, PDF, CSV, XML ed Excel.

Navigazione verso report predefiniti

Quando si apre il portale di reporting, la cartella *Team Content* è il punto di partenza per selezionare il tipo di informazioni necessarie nei report di Data Infrastructure Insights .

1. Nel riquadro di navigazione a sinistra, seleziona **Contenuto > Contenuto del team**.
2. Selezionare **Report** per accedere ai report predefiniti.





Utilizzo di report predefiniti per rispondere a domande comuni

I seguenti report predefiniti sono disponibili in **Contenuto del team > Report**.

Capacità e prestazioni del livello di servizio dell'applicazione

Il report Capacità e prestazioni del livello di servizio dell'applicazione fornisce una panoramica di alto livello delle tue applicazioni. È possibile utilizzare queste informazioni per la pianificazione della capacità o per un piano di migrazione.

Riaddebito

Il report Chargeback fornisce informazioni sulla capacità di storage chargeback e sulla responsabilità per host, applicazione ed entità aziendali e include sia dati attuali che storici.

Per evitare doppi conteggi, non includere i server ESX, ma monitorare solo le VM.

Fonti dei dati

Il report Origini dati mostra tutte le origini dati installate sul tuo sito, lo stato dell'origine dati (esito positivo/negativo) e i messaggi di stato. Il report fornisce informazioni su dove iniziare la risoluzione dei problemi relativi alle fonti di dati. Le fonti di dati non valide incidono sull'accuratezza dei report e sull'usabilità generale del prodotto.

Prestazioni ESX vs VM

Il report sulle prestazioni ESX vs VM fornisce un confronto tra server ESX e VM, mostrando IOPS medi e di picco, throughput, latenza e utilizzi per server ESX e VM. Per evitare doppi conteggi, escludere i server ESX e includere solo le VM. Una versione aggiornata di questo report è disponibile nel NetApp Storage Automation Store.

Riepilogo del tessuto

Il report Riepilogo Fabric identifica gli switch e le relative informazioni, tra cui il numero di porte, le versioni del firmware e lo stato della licenza. Il rapporto non include le porte switch NPV.

HBA ospitanti

Il report HBA host fornisce una panoramica degli host nell'ambiente e indica il fornitore, il modello e la versione firmware degli HBA, nonché il livello firmware degli switch a cui sono collegati. Questo report può essere utilizzato per analizzare la compatibilità del firmware quando si pianifica un aggiornamento del firmware per uno switch o un HBA.

Capacità e prestazioni del livello di servizio host

Il report Capacità e prestazioni del livello di servizio host fornisce una panoramica dell'utilizzo dello storage da parte dell'host per le applicazioni solo a blocchi.

Riepilogo dell'host

Il report Riepilogo host fornisce una panoramica dell'utilizzo dello storage da parte di ciascun host selezionato, con informazioni sugli host Fibre Channel e iSCSI. Il report consente di confrontare porte e percorsi, capacità Fibre Channel e ISCSI e conteggi delle violazioni.

Dettagli della licenza

Il report Dettagli licenza mostra la quantità di risorse autorizzate per le quali si dispone di licenza su tutti i siti con licenze attive. Il report mostra anche una sintesi della quantità effettiva in tutti i siti con licenze attive. La somma può includere sovrapposizioni di array di archiviazione gestiti da più server.

Volumi mappati ma non mascherati

Il report Volumi mappati ma non mascherati elenca i volumi il cui numero di unità logica (LUN) è stato mappato per l'utilizzo da parte di un host specifico, ma non è mascherato per quell'host. In alcuni casi potrebbero trattarsi di LUN dismesse che sono state smascherate. I volumi non mascherati sono accessibili a qualsiasi host, il che li rende vulnerabili al danneggiamento dei dati.

Capacità e prestazioni NetApp

Il report Capacità e prestazioni NetApp fornisce dati globali sulla capacità allocata, utilizzata e impegnata, con dati sulle tendenze e sulle prestazioni per la capacità NetApp .

Scheda di valutazione

Il report Scorecard fornisce un riepilogo e lo stato generale di tutte le risorse acquisite da Data Infrastructure Insights. Lo stato è indicato con bandiere verdi, gialle e rosse:

- Il verde indica condizioni normali
- Il giallo indica un potenziale problema nell'ambiente
- Il rosso indica un problema che richiede attenzione

Tutti i campi del report sono descritti nel dizionario dati fornito con il report.

Riepilogo archiviazione

Il report Riepilogo archiviazione fornisce un riepilogo globale dei dati sulla capacità utilizzata e non utilizzata per volumi, pool di archiviazione e dati grezzi e allocati. Questo report fornisce una panoramica di tutti gli archivi scoperti.

Capacità e prestazioni della VM

Descrive l'ambiente della macchina virtuale (VM) e il suo utilizzo della capacità. Per visualizzare alcuni dati, ad esempio quando le VM sono state spente, è necessario abilitare gli strumenti VM.

Percorsi VM

Il report Percorsi VM fornisce dati sulla capacità dell'archivio dati e metriche sulle prestazioni per sapere quale macchina virtuale è in esecuzione su quale host, quali host accedono a quali volumi condivisi, qual è il

percorso di accesso attivo e cosa comprende l'allocazione e l'utilizzo della capacità.

Capacità HDS tramite Thin Pool

Il report Capacità HDS per Thin Pool mostra la quantità di capacità utilizzabile su uno storage pool sottoposto a thin provisioning.

Capacità NetApp per aggregato

Il report Capacità NetApp per aggregato mostra lo spazio totale grezzo, totale, utilizzato, disponibile e impegnato degli aggregati.

Capacità Symmetrix per Thick Array

Il report Capacità Symmetrix per Thick Array mostra la capacità grezza, la capacità utilizzabile, la capacità libera, la capacità mappata, quella mascherata e la capacità libera totale.

Capacità Symmetrix di Thin Pool

Il report Capacità Symmetrix per Thin Pool mostra la capacità grezza, la capacità utilizzabile, la capacità utilizzata, la capacità libera, la percentuale utilizzata, la capacità sottoscritta e la frequenza di sottoscrizione.

XIV Capacità per Array

Il report XIV Capacità per array mostra la capacità utilizzata e non utilizzata per l'array.

XIV Capacità per piscina

Il report XIV Capacità per pool mostra la capacità utilizzata e non utilizzata per i pool di archiviazione.

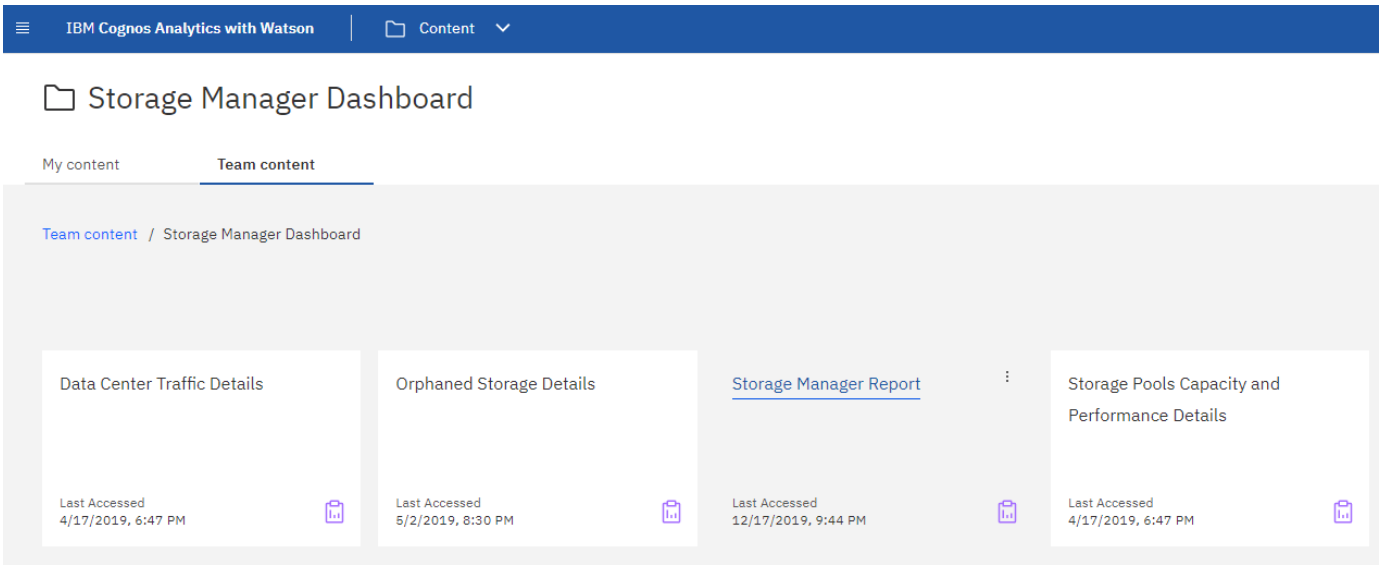
Dashboard del gestore dell'archiviazione

La dashboard di Storage Manager fornisce una visualizzazione centralizzata che consente di confrontare e contrapporre l'utilizzo delle risorse nel tempo rispetto agli intervalli accettabili e ai giorni di attività precedenti. Visualizzando solo le metriche chiave delle prestazioni per i tuoi servizi di archiviazione, puoi prendere decisioni su come gestire i tuoi data center.

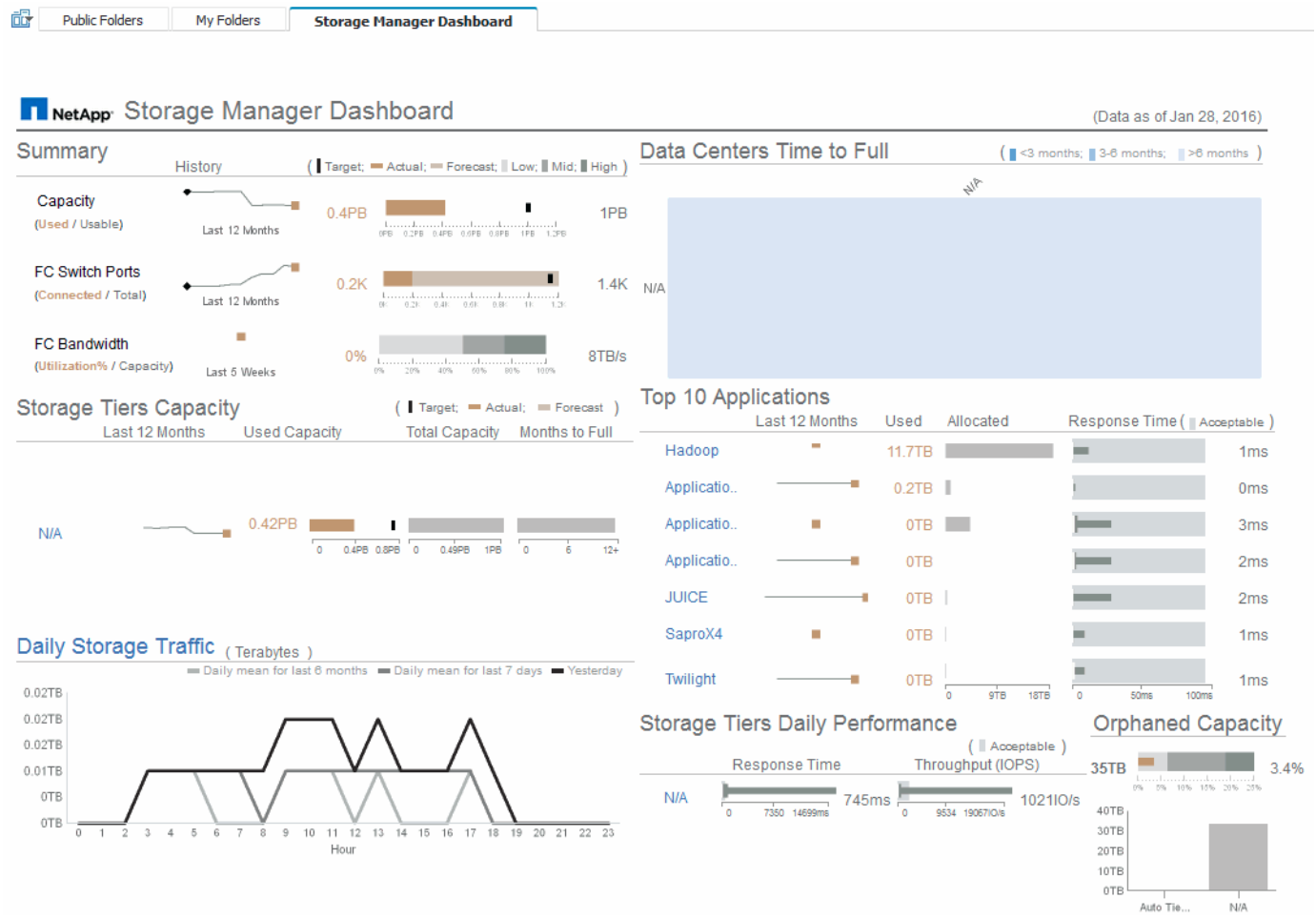
La funzionalità di reporting è disponibile in Data Infrastructure Insights"Edizione Premium" .

Riepilogo

Selezionando **Storage Manager Dashboard** da Team Content vengono visualizzati diversi report che forniscono informazioni sul traffico e sullo spazio di archiviazione.



Per una panoramica immediata, il **Storage Manager Report** è composto da sette componenti che contengono informazioni contestuali su numerosi aspetti dell'ambiente di archiviazione. Puoi approfondire gli aspetti dei tuoi servizi di archiviazione per eseguire un'analisi approfondita della sezione che più ti interessa.



Questo componente mostra la capacità di archiviazione utilizzata rispetto a quella utilizzabile, il numero totale di porte switch rispetto al numero di porte switch connesse e l'utilizzo totale delle porte switch connesse rispetto alla larghezza di banda totale, nonché l'andamento di ciascuno di questi nel tempo. È possibile visualizzare l'utilizzo effettivo confrontandolo con i valori basso, medio e alto, consentendo di confrontare e

contrapporre l'utilizzo tra le proiezioni e i valori effettivi desiderati, in base a un obiettivo. Per capacità e porte switch, è possibile configurare questa destinazione. La previsione si basa su un'estrapolazione del tasso di crescita attuale e della data impostata. Quando la capacità utilizzata prevista, basata sulla data di proiezione dell'utilizzo futuro, supera l'obiettivo, accanto a Capacità viene visualizzato un avviso (cerchio rosso pieno).

Capacità dei livelli di archiviazione

Questo componente mostra la capacità di livello utilizzata rispetto alla capacità assegnata al livello, che indica come la capacità utilizzata aumenta o diminuisce in un periodo di 12 mesi e quanti mesi rimangono per raggiungere la piena capacità. L'utilizzo della capacità viene mostrato con valori forniti per l'utilizzo effettivo, la previsione di utilizzo e un obiettivo per la capacità, che è possibile configurare. Quando la capacità utilizzata prevista, basata sulla data di proiezione dell'utilizzo futuro, supera la capacità target, accanto a un livello viene visualizzato un avviso (cerchio rosso pieno).

È possibile fare clic su qualsiasi livello per visualizzare il report Dettagli capacità e prestazioni dei pool di archiviazione, che mostra le capacità libere rispetto a quelle utilizzate, il numero di giorni mancanti al riempimento e i dettagli sulle prestazioni (IOPS e tempo di risposta) per tutti i pool nel livello selezionato. È anche possibile fare clic su qualsiasi nome di storage o pool di storage in questo report per visualizzare la pagina delle risorse che riassume lo stato corrente di tale risorsa.

Traffico di archiviazione giornaliero

Questo componente mostra le prestazioni dell'ambiente, se si sono verificate grandi crescite, cambiamenti o potenziali problemi rispetto ai sei mesi precedenti. Mostra anche il traffico medio rispetto al traffico dei sette giorni precedenti e del giorno precedente. È possibile visualizzare eventuali anomalie nelle prestazioni dell'infrastruttura, poiché fornisce informazioni che evidenziano sia le variazioni cicliche (sette giorni precedenti) sia quelle stagionali (sei mesi precedenti).

È possibile fare clic sul titolo (Traffico di archiviazione giornaliero) per visualizzare il report Dettagli traffico di archiviazione, che mostra la mappa termica del traffico di archiviazione orario del giorno precedente per ciascun sistema di archiviazione. Fare clic su un nome di archiviazione in questo report per visualizzare la pagina delle risorse che riassume lo stato corrente di tale risorsa.

Tempo di completamento dei data center

Questo componente mostra tutti i data center rispetto a tutti i livelli e quanta capacità rimane in ciascun data center per ciascun livello di storage in base ai tassi di crescita previsti. Il livello di capacità del livello è mostrato in blu; più scuro è il colore, minore è il tempo rimanente prima che il livello nella posizione sia pieno.

È possibile fare clic su una sezione di un livello per visualizzare il report Dettagli giorni mancanti al riempimento dei pool di archiviazione, che mostra la capacità totale, la capacità libera e il numero di giorni mancanti al riempimento per tutti i pool nel livello selezionato e nel data center. Fare clic su qualsiasi nome di storage o pool di storage in questo report per visualizzare la pagina delle risorse che riassume lo stato corrente di tale risorsa.

Le 10 migliori applicazioni

Questo componente mostra le 10 applicazioni principali in base alla capacità utilizzata. Indipendentemente dal modo in cui il livello organizza i dati, quest'area mostra la capacità attualmente utilizzata e la quota dell'infrastruttura. È possibile visualizzare l'intervallo di esperienza utente nei sette giorni precedenti per verificare se i consumatori hanno riscontrato tempi di risposta accettabili (o, cosa più importante, inaccettabili).

Quest'area mostra anche le tendenze, che indicano se le applicazioni soddisfano i loro obiettivi di livello di servizio (SLO) in termini di prestazioni. È possibile visualizzare il tempo di risposta minimo della settimana precedente, il primo quartile, il terzo quartile e il tempo di risposta massimo, con una mediana visualizzata

rispetto a un SLO accettabile, che è possibile configurare. Quando il tempo di risposta mediano per un'applicazione non rientra nell'intervallo SLO accettabile, accanto all'applicazione viene visualizzato un avviso (cerchio rosso pieno). È possibile fare clic su un'applicazione per visualizzare la pagina delle risorse che riassume lo stato attuale di tale risorsa.

Livelli di archiviazione - Prestazioni giornaliere

Questo componente mostra un riepilogo delle prestazioni del livello in termini di tempo di risposta e IOPS per i sette giorni precedenti. Queste prestazioni vengono confrontate con uno SLO, che è possibile configurare, consentendo di verificare se è possibile consolidare i livelli, riallineare i carichi di lavoro forniti da tali livelli o identificare problemi con livelli specifici. Quando il tempo di risposta mediano o l'IOPS mediano non rientrano nell'intervallo SLO accettabile, accanto a un livello viene visualizzato un avviso (cerchio rosso pieno).

È possibile fare clic sul nome di un livello per visualizzare il report Dettagli capacità e prestazioni dei pool di archiviazione, che mostra le capacità libere rispetto a quelle utilizzate, il numero di giorni mancanti al riempimento e i dettagli sulle prestazioni (IOPS e tempo di risposta) per tutti i pool nel livello selezionato. Fare clic su qualsiasi archivio o pool di archiviazione in questo report per visualizzare la pagina delle risorse che riassume lo stato corrente di tale risorsa.

Capacità orfana

Questo componente mostra la capacità orfana totale e la capacità orfana per livello, confrontandola con intervalli accettabili per la capacità totale utilizzabile e mostrando la capacità effettiva orfana. La capacità orfana è definita dalla configurazione e dalle prestazioni. L'archiviazione orfana per configurazione descrive una situazione in cui è presente spazio di archiviazione allocato a un host. Tuttavia, la configurazione non è stata eseguita correttamente e l'host non riesce ad accedere allo storage. L'archiviazione è orfana in termini di prestazioni quando è correttamente configurata per essere accessibile da un host. Tuttavia, non si è verificato alcun traffico di archiviazione.

La barra orizzontale sovrapposta mostra gli intervalli accettabili. Più scuro è il grigio, più inaccettabile è la situazione. La situazione reale è mostrata dalla barra stretta in bronzo che indica la capacità effettivamente rimasta orfana.

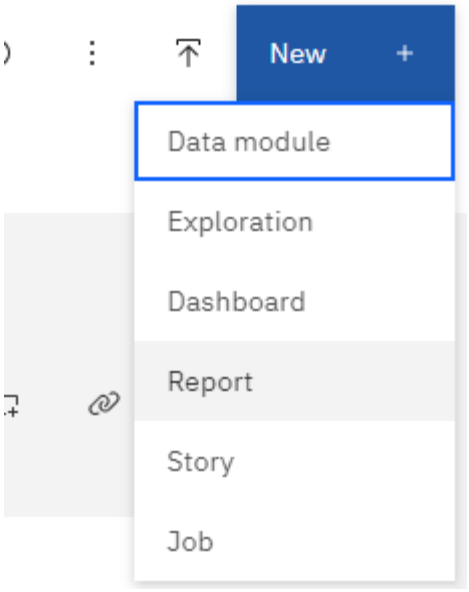
È possibile fare clic su un livello per visualizzare il report Dettagli archiviazione orfani, che mostra tutti i volumi identificati come orfani in base alla configurazione e alle prestazioni per il livello selezionato. Fare clic su qualsiasi archivio, pool di archiviazione o volume in questo report per visualizzare la pagina delle risorse che riassume lo stato corrente di tale risorsa.

Creazione di un report (esempio)

Utilizzare i passaggi di questo esempio per generare un semplice report sulla capacità fisica dello storage e dei pool di storage in diversi data center.

Passi

1. Vai a **Menu > Contenuto > Contenuto del team > Report**
2. In alto a destra dello schermo, seleziona **[Nuovo +]**
3. Seleziona **Segnala**



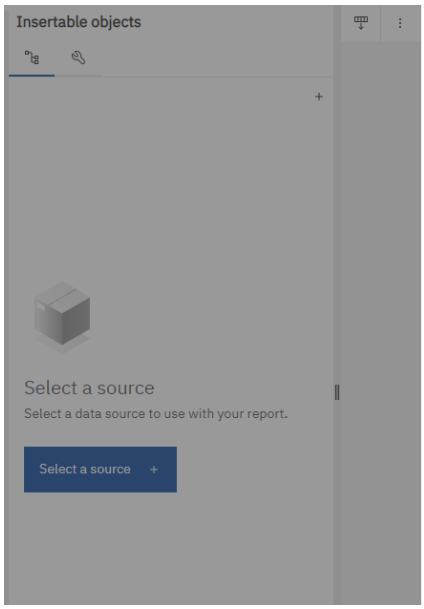
4. Nella scheda **Modelli**, seleziona *Vuoto*

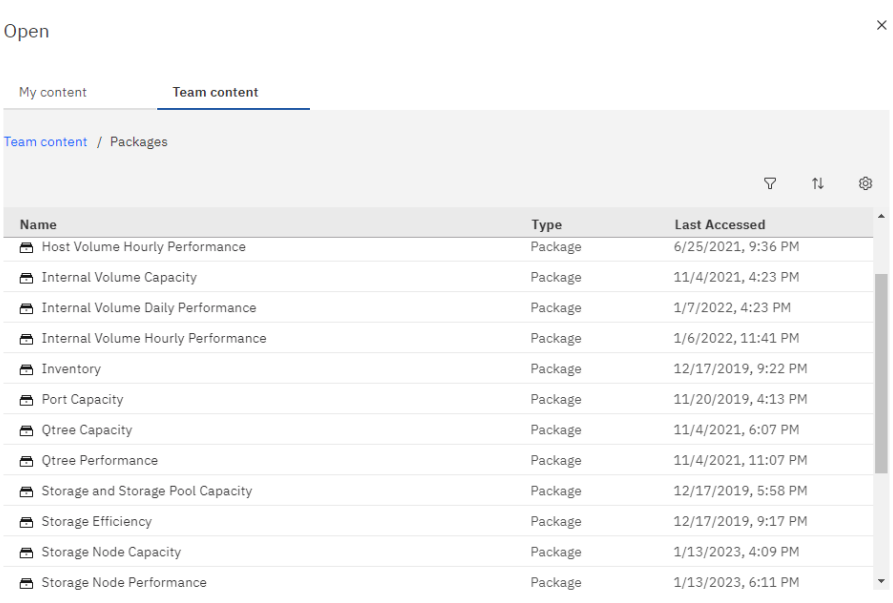
   Vengono visualizzate le schede Origine e Dati

5. Apri **Seleziona una fonte +**
6. In **Contenuto del team**, apri **Pacchetti**

   Viene visualizzato un elenco dei pacchetti disponibili.

7. Scegli *Capacità di archiviazione e pool di archiviazione*





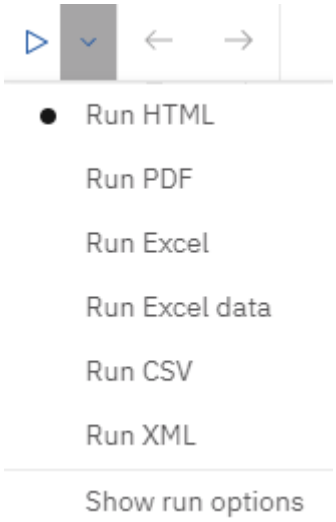
8. Seleziona **Apri**

   Vengono visualizzati gli stili disponibili per il report.

9. Seleziona **Elenco**

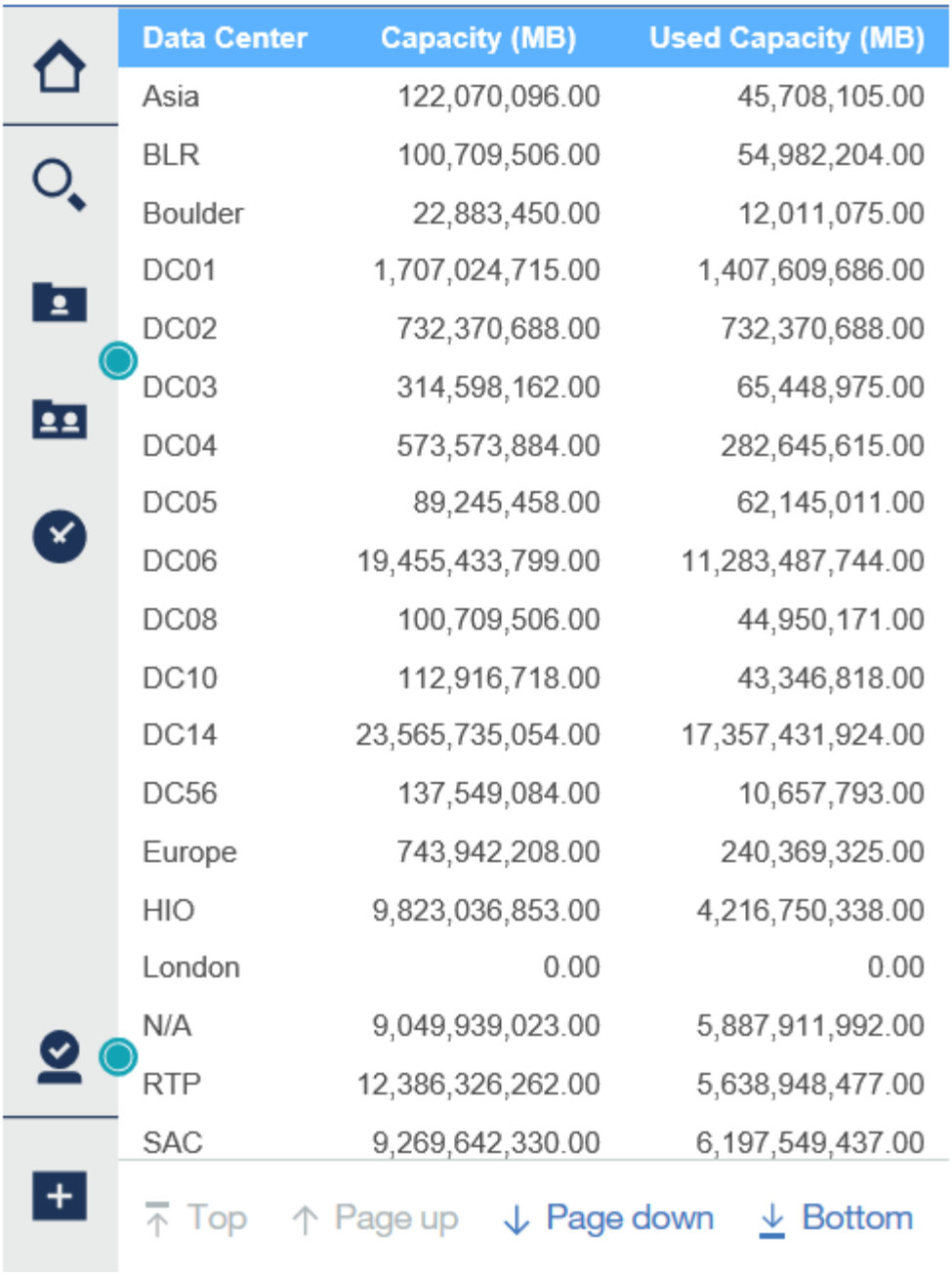
   Aggiungi nomi appropriati per Elenco e Query

10. Seleziona **OK**
11. Espandi *Capacità fisica*
12. Espandere al livello più basso del *Data Center*
13. Trascina *Data Center* nel riquadro Report.
14. Espandi *Capacità (MB)*
15. Trascina *Capacità (MB)* nel riquadro Report.
16. Trascina *Capacità utilizzata (MB)* nel riquadro Report.
17. Eseguire il report selezionando un tipo di output dal menu **Esegui**.



Risultato

Viene creato un report simile al seguente:



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

Gestione dei report

È possibile personalizzare il formato di output e la consegna di un report, impostare le proprietà o le pianificazioni del report e inviare i report tramite e-mail.

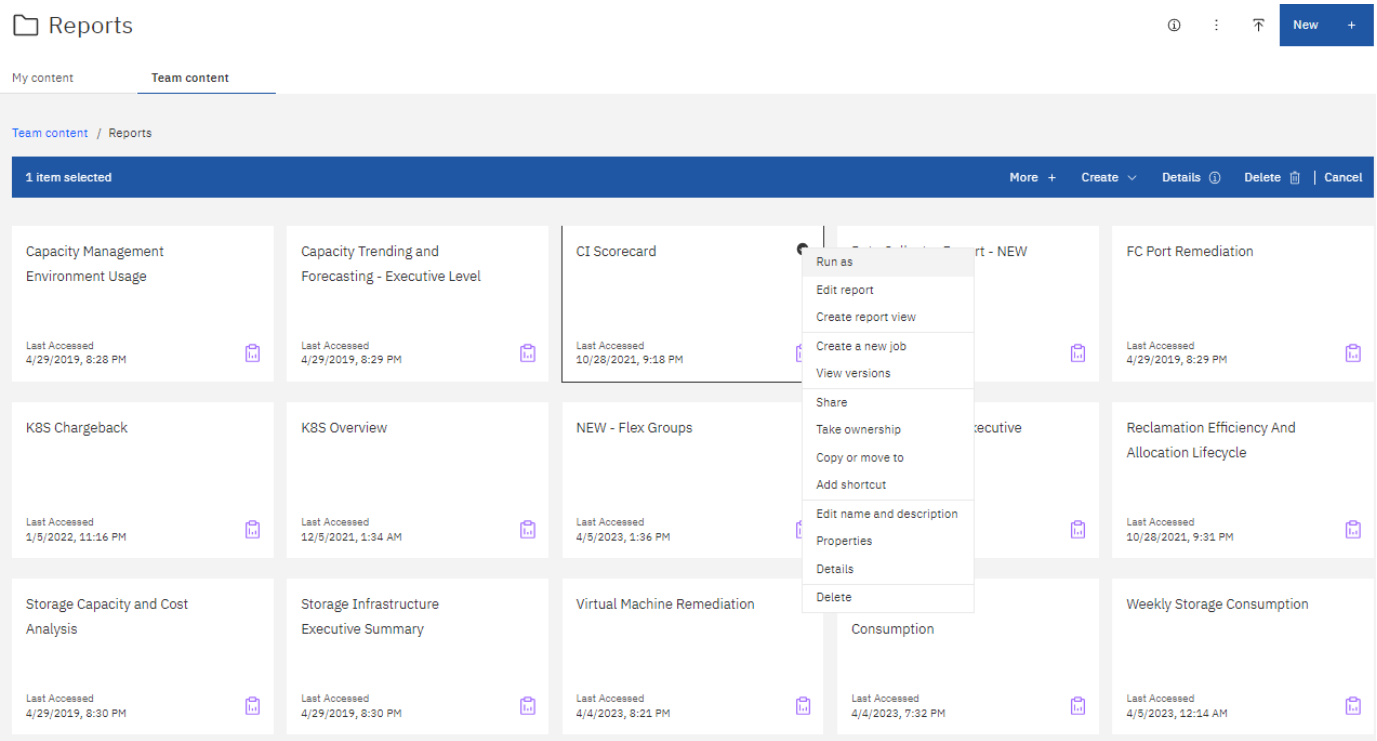
La funzionalità di reporting è disponibile in Data Infrastructure Insights"Edizione Premium" .

Prima di apportare modifiche alle autorizzazioni di reporting o alla sicurezza, è necessario copiare i report "I miei contenuti" nella cartella "Contenuti del team" per assicurarsi che i report vengano salvati.

Personalizzazione del formato di output e della consegna di un report

È possibile personalizzare il formato e il metodo di consegna dei report.

1. Nel portale di reporting di Data Infrastructure Insights , vai a **Menu > Contenuto > Contenuto personale/Contenuto del team**. Passa il mouse sul report che vuoi personalizzare e apri il menu "tre punti".

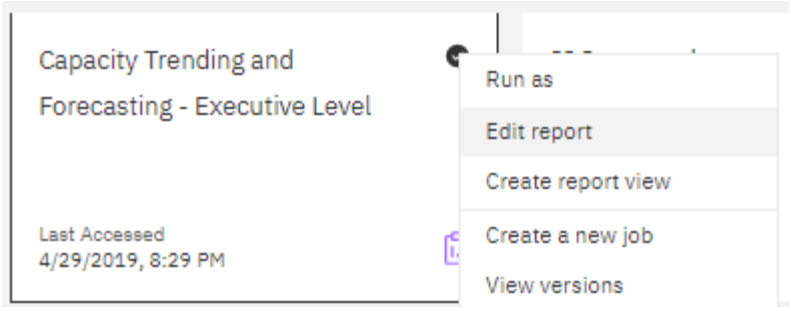


1. Fare clic su **Proprietà > Pianificazione**
2. È possibile impostare le seguenti opzioni:
   - **Pianifica** quando vuoi che i report vengano eseguiti.
   - Selezionare **Opzioni** per il formato e la consegna del report (Salva, Stampa, E-mail) e le lingue per il report.
3. Fare clic su **Salva** per produrre il report utilizzando le selezioni effettuate.

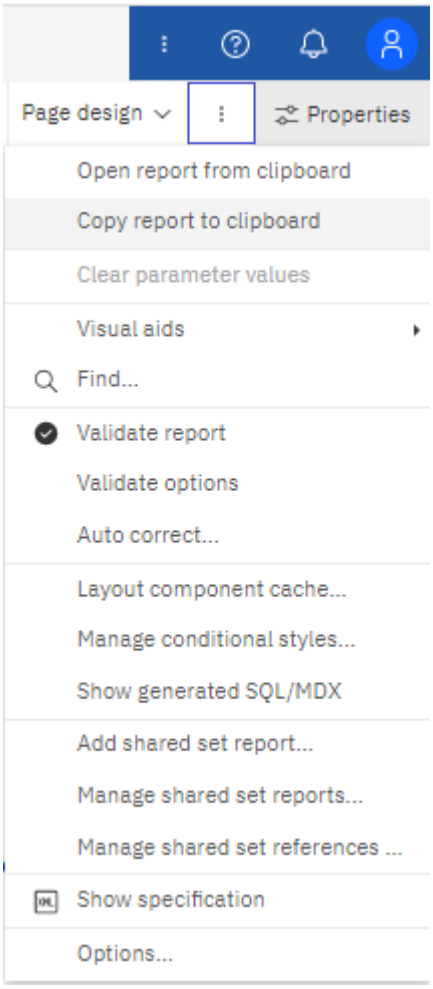
Copia di un report negli appunti

Utilizzare questa procedura per copiare un report negli appunti.

1. Seleziona un report da cui copiare (**Menu > Contenuto > Il mio contenuto o Contenuto del team**)
2. Seleziona *Modifica report* dal menu a discesa del report



3. Nell'angolo in alto a destra dello schermo, apri il menu "tre puntini" accanto a "Proprietà".
4. Selezionare **Copia report negli appunti**.

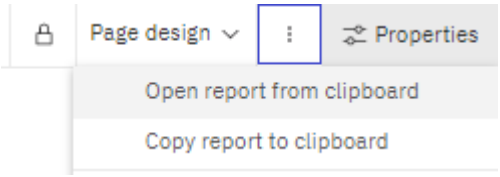


Apertura dei report dagli appunti

È possibile aprire una specifica del report precedentemente copiata negli appunti.

Informazioni su questa attività Inizia creando un nuovo report o aprendo un report esistente che desideri sostituire con il report copiato. I passaggi seguenti sono per un nuovo report.

1. Selezionare **Menu > +Nuovo > Report** e creare un report vuoto.
2. Nell'angolo in alto a destra dello schermo, apri il menu "tre puntini" accanto a "Proprietà".
3. Selezionare **Apri report dagli appunti**.



1. Incolla il codice copiato nella finestra e seleziona **OK**.
2. Selezionare l'icona del floppy disk per salvare il report.
3. Scegli dove salvare il report (*I miei contenuti*, *Contenuti del team* o crea una nuova cartella).
4. Assegna un nome significativo al nuovo report e seleziona **Salva**.

Modifica di un report esistente

Tieni presente che la modifica dei file nella loro posizione predefinita comporta il rischio che i report vengano sovrascritti al successivo aggiornamento del catalogo dei report. Si consiglia di salvare il report modificato con un nuovo nome o di memorizzarlo in una posizione diversa da quella predefinita.

Risoluzione dei problemi

Qui troverete suggerimenti per la risoluzione dei problemi relativi alla segnalazione.

Problema:	Prova questo:
Quando si pianifica l'invio di un report tramite e-mail, il nome dell'utente che ha effettuato l'accesso viene precompilato nel campo "A" dell'e-mail. Tuttavia, il nome è nella forma "nome cognome" (nome, spazio, cognome). Poiché non si tratta di un indirizzo email valido, l'email non verrà inviata quando verrà eseguito il report pianificato.	Quando si pianifica l'invio del report tramite e-mail, cancellare il nome precompilato e immettere un indirizzo e-mail valido e formattato correttamente nel campo "A".
Il mio report programmato viene inviato via e-mail, ma non è possibile accedervi se l'origine è la cartella "I miei contenuti".	Per evitare ciò, il report o la visualizzazione del report devono essere salvati nella cartella **Contenuto del team › Report personalizzati - xxxxxx** e la pianificazione deve essere creata da quella versione salvata. La cartella "Report personalizzati - xxxxxx" è visibile a tutti gli utenti del tenant.
quando si salva un lavoro, la cartella potrebbe mostrare "Contenuto del team" con l'elenco del contenuto da "Report personalizzati - xxxxxx", tuttavia non è possibile salvare il lavoro qui perché Cognos ritiene che questa sia la cartella "Contenuto del team" in cui non si ha accesso in scrittura.	La soluzione alternativa è creare una nuova cartella con un nome univoco (ad esempio "NewFolder") e salvarla lì, oppure salvarla in "My Content" e poi copiarla/spostarla in "Custom Reports - xxxxxx".

Creazione di report personalizzati

È possibile utilizzare gli strumenti di creazione dei report per creare report personalizzati. Dopo aver creato i report, è possibile salvarli ed eseguirli regolarmente. I risultati dei report possono essere inviati automaticamente via e-mail a te stesso e ad altri.

La funzionalità di reporting è disponibile in Data Infrastructure Insights"Edizione Premium" .

Gli esempi in questa sezione mostrano il seguente processo, che può essere utilizzato per qualsiasi modello di dati di Data Infrastructure Insights Reporting:

- Identificare una domanda a cui rispondere con un report
- Determinazione dei dati necessari a supporto dei risultati
- Selezione degli elementi dati per il report

Prima di progettare il tuo report personalizzato, devi completare alcune attività preliminari. Se non si compilano queste informazioni, i report potrebbero risultare inaccurati o incompleti.

Ad esempio, se non si completa il processo di identificazione del dispositivo, i report sulla capacità non saranno accurati. Oppure, se non completi l'impostazione delle annotazioni (ad esempio livelli, unità aziendali e data center), i tuoi report personalizzati potrebbero non riportare accuratamente i dati nel tuo dominio o potrebbero mostrare "N/D" per alcuni punti dati.

Prima di progettare i report, completa le seguenti attività:

- Configura tutto"raccoglitori di dati" correttamente.
- Inserisci annotazioni (ad esempio livelli, data center e unità aziendali) sui dispositivi e sulle risorse del tuo tenant. È utile disporre di annotazioni stabili prima di generare report, perché Data Infrastructure Insights Reporting raccoglie informazioni storiche.

Processo di creazione del report

Il processo di creazione di report personalizzati (chiamati anche "ad hoc") prevede diverse attività:

- Pianifica i risultati del tuo report.
- Identifica i dati a supporto dei tuoi risultati.
- Selezionare il modello di dati (ad esempio, modello di dati di addebito, modello di dati di inventario e così via) che contiene i dati.
- Selezionare gli elementi dati per il report.
- Facoltativamente, formattare, ordinare e filtrare i risultati del report.

Pianificazione dei risultati del report personalizzato

Prima di aprire gli strumenti di creazione del report, potrebbe essere opportuno pianificare i risultati che si desidera ottenere dal report. Con gli strumenti di creazione di report, è possibile creare report facilmente e potrebbe non essere necessaria una grande pianificazione; tuttavia, è una buona idea chiedere al richiedente del report quali siano i requisiti del report.

- Individua la domanda esatta a cui vuoi rispondere. Per esempio:
  - Quanta capacità mi rimane?
  - Quali sono i costi di chargeback per unità aziendale?
  - Qual è la capacità per livello per garantire che le unità aziendali siano allineate al livello di archiviazione appropriato?
  - Come posso prevedere i requisiti di alimentazione e raffreddamento? (Aggiungi metadati personalizzati inserendo annotazioni alle risorse.)
- Identifica gli elementi dati necessari a supportare la risposta.
- Identifica le relazioni tra i dati che vuoi vedere nella risposta. Non includere relazioni illogiche nella tua

domanda, ad esempio "Voglio vedere le porte correlate alla capacità".

- Identificare eventuali calcoli necessari sui dati.
- Determinare quali tipi di filtraggio sono necessari per limitare i risultati.
- Determina se devi utilizzare dati attuali o storici.
- Determina se è necessario impostare privilegi di accesso sui report per limitare i dati a un pubblico specifico.
- Definire come verrà distribuito il report. Ad esempio, dovrebbe essere inviato tramite e-mail secondo una pianificazione prestabilita o incluso nell'area della cartella dei contenuti del team?
- Stabilire chi si occuperà della manutenzione del rapporto. Ciò potrebbe influire sulla complessità del progetto.
- Creare un mockup del report.

Suggerimenti per la progettazione di report

Quando si progettano report, potrebbero essere utili alcuni suggerimenti.

- Determina se devi utilizzare dati attuali o storici.

  La maggior parte dei report deve riportare solo i dati più recenti disponibili in Data Infrastructure Insights.

- Data Infrastructure Insights Reporting fornisce informazioni storiche sulla capacità e sulle prestazioni, ma non sull'inventario.
- Tutti possono vedere tutti i dati; tuttavia, potrebbe essere necessario limitare i dati a un pubblico specifico.

  Per segmentare le informazioni per diversi utenti, è possibile creare report e impostare per ciascuno di essi le autorizzazioni di accesso.

Modelli di dati di reporting

Data Infrastructure Insights include diversi modelli di dati dai quali è possibile selezionare report predefiniti o creare report personalizzati.

Ogni modello di dati contiene un data mart semplice e un data mart avanzato:

- Il data mart semplice fornisce un rapido accesso agli elementi dati più comunemente utilizzati e include solo l'ultima istantanea dei dati del Data Warehouse; non include dati storici.
- Il data mart avanzato fornisce tutti i valori e i dettagli disponibili nel data mart semplice e include l'accesso ai valori dei dati storici.

Modelli di dati di capacità

Consente di rispondere a domande sulla capacità di archiviazione, sull'utilizzo del file system, sulla capacità del volume interno, sulla capacità delle porte, sulla capacità di qtree e sulla capacità della macchina virtuale (VM). Il modello di dati di capacità è un contenitore per diversi modelli di dati di capacità. Utilizzando questo modello di dati è possibile creare report che rispondano a vari tipi di domande:

Modello di dati di archiviazione e capacità del pool di archiviazione

Consente di rispondere a domande sulla pianificazione delle risorse di capacità di archiviazione, inclusi storage e pool di archiviazione, e include dati di pool di archiviazione sia fisici che virtuali. Questo semplice

modello di dati può aiutarti a rispondere a domande relative alla capacità sul pavimento e all'utilizzo della capacità dei pool di archiviazione per livello e data center nel tempo. Se non hai familiarità con i report sulla capacità, dovresti iniziare con questo modello di dati perché è un modello di dati più semplice e mirato. Utilizzando questo modello di dati è possibile rispondere a domande simili alle seguenti:

- Qual è la data prevista per il raggiungimento della soglia di capacità dell'80% del mio spazio di archiviazione fisico?
- Qual è la capacità di archiviazione fisica di un array per un dato livello?
- Qual è la mia capacità di archiviazione in base al produttore, alla famiglia e al data center?
- Qual è l'andamento dell'utilizzo dello storage su un array per tutti i livelli?
- Quali sono i miei 10 sistemi di storage con il maggiore utilizzo?
- Qual è l'andamento dell'utilizzo dello storage nei pool di storage?
- Quanta capacità è già stata assegnata?
- Quale capacità è disponibile per l'assegnazione?

Modello di dati di utilizzo del file system

Questo modello di dati fornisce visibilità sull'utilizzo della capacità da parte degli host a livello di file system. Gli amministratori possono determinare la capacità allocata e utilizzata per ogni file system, determinare il tipo di file system e identificare le statistiche di tendenza in base al tipo di file system. Utilizzando questo modello di dati è possibile rispondere alle seguenti domande:

- Qual è la dimensione del file system?
- Dove vengono conservati i dati e come vengono consultati, ad esempio in locale o in SAN?
- Quali sono le tendenze storiche per la capacità del file system? Quindi, sulla base di ciò, cosa possiamo prevedere per le esigenze future?

Modello di dati di capacità del volume interno

Consente di rispondere a domande sulla capacità utilizzata del volume interno, sulla capacità assegnata e sull'utilizzo della capacità nel tempo:

- Quali volumi interni hanno un utilizzo superiore a una soglia predefinita?
- Quali volumi interni rischiano di esaurire la capacità in base a un trend? 8 Qual è la capacità utilizzata rispetto alla capacità assegnata sui nostri volumi interni?

Modello di dati sulla capacità del porto

Consente di rispondere a domande sulla connettività delle porte dello switch, sullo stato delle porte e sulla velocità delle porte nel tempo. Puoi rispondere a domande simili alle seguenti per aiutarti a pianificare l'acquisto di nuovi switch: Come posso creare una previsione del consumo di porte che preveda la disponibilità delle risorse (porte) (in base al data center, al fornitore dello switch e alla velocità della porta)?

- Quali porte rischiano di esaurire la loro capacità, in base alla velocità dei dati, al data center, al fornitore e al numero di porte host e di archiviazione?
- Quali sono le tendenze nel tempo della capacità delle porte degli switch?
- Quali sono le velocità delle porte?
- Quale tipo di capacità portuale è necessaria e quale organizzazione sta per esaurire un certo tipo di porto o fornitore?

- Qual è il momento ottimale per acquistare tale capacità e renderla disponibile?

Modello di dati di capacità Qtree

Consente di tracciare l'andamento dell'utilizzo di qtree (con dati quali la capacità utilizzata rispetto a quella assegnata) nel tempo. È possibile visualizzare le informazioni in base a diverse dimensioni, ad esempio per entità aziendale, applicazione, livello e livello di servizio. Utilizzando questo modello di dati è possibile rispondere alle seguenti domande:

- Qual è la capacità utilizzata per i qtree rispetto ai limiti impostati per applicazione o entità aziendale?
- Quali sono le tendenze della nostra capacità utilizzata e libera in modo da poter pianificare la capacità?
- Quali entità aziendali stanno utilizzando la maggiore capacità?
- Quali applicazioni consumano più capacità?

Modello di dati di capacità della VM

Consente di segnalare l'ambiente virtuale e l'utilizzo della sua capacità. Questo modello di dati consente di segnalare le variazioni nell'utilizzo della capacità nel tempo per VM e archivi dati. Il modello di dati fornisce anche dati di thin provisioning e di chargeback delle macchine virtuali.

- Come posso determinare il chargeback della capacità in base alla capacità fornita alle VM e agli archivi dati?
- Quale capacità non viene utilizzata dalle VM e quale parte inutilizzata è libera, orfana o altro?
- Cosa dobbiamo acquistare in base alle tendenze di consumo?
- Quali risparmi in termini di efficienza di storage si ottengono utilizzando le tecnologie di thin provisioning e deduplicazione dello storage?

Le capacità nel modello di dati VM Capacity vengono ricavate dai dischi virtuali (VMDK). Ciò significa che la dimensione fornita di una VM utilizzando il modello di dati Capacità VM è la dimensione dei suoi dischi virtuali. Questa è diversa dalla capacità fornita nella vista Macchine virtuali in Data Infrastructure Insights, che mostra la dimensione fornita per la VM stessa.

Modello di dati di capacità del volume

Consente di analizzare tutti gli aspetti dei volumi sul tenant e di organizzare i dati in base a fornitore, modello, livello, livello di servizio e data center.

È possibile visualizzare la capacità relativa ai volumi orfani, ai volumi inutilizzati e ai volumi di protezione (utilizzati per la replica). È inoltre possibile visualizzare diverse tecnologie di volume (iSCSI o FC) e confrontare volumi virtuali con volumi non virtuali per problemi di virtualizzazione degli array.

Con questo modello di dati puoi rispondere a domande simili alle seguenti:

- Quali volumi hanno un utilizzo superiore a una soglia predefinita?
- Qual è la tendenza nel mio data center per quanto riguarda la capacità dei volumi orfani?
- Quanta capacità del mio data center è virtualizzata o sottoposta a thin provisioning?
- Quanta capacità del mio data center deve essere riservata alla replica?

Modello di dati di addebito

Consente di rispondere a domande sulla capacità utilizzata e sulla capacità allocata sulle risorse di archiviazione (volumi, volumi interni e qtree). Questo modello di dati fornisce informazioni sulla capacità di storage e sulla responsabilità per host, applicazioni ed entità aziendali e include sia dati attuali che storici. I dati del report possono essere classificati in base al livello di servizio e al livello di archiviazione.

È possibile utilizzare questo modello di dati per generare report di addebito in conto individuando la quantità di capacità utilizzata da un'entità aziendale. Questo modello di dati consente di creare report unificati di più protocolli (tra cui NAS, SAN, FC e iSCSI).

- Per l'archiviazione senza volumi interni, i report di addebito mostrano l'addebito in base ai volumi.
- Per l'archiviazione con volumi interni:
  - Se le entità aziendali sono assegnate ai volumi, i report di addebito mostrano l'addebito in base ai volumi.
  - Se le entità aziendali non sono assegnate ai volumi ma ai qtree, i report di addebito mostrano l'addebito per qtree.
  - Se le entità aziendali non sono assegnate a volumi e non sono assegnate a qtree, i report di addebito mostrano il volume interno.
  - La decisione se visualizzare il chargeback per volume, qtree o volume interno viene presa per ciascun volume interno, quindi è possibile che diversi volumi interni nello stesso pool di archiviazione visualizzino il chargeback a livelli diversi.

I dati sulla capacità vengono eliminati dopo un intervallo di tempo predefinito. Per maggiori dettagli, vedere Processi del Data Warehouse.

I report che utilizzano il modello dati Chargeback potrebbero visualizzare valori diversi rispetto ai report che utilizzano il modello dati Storage Capacity.

- Per gli array di storage che non sono sistemi di storage NetApp , i dati di entrambi i modelli di dati sono gli stessi.
- Per i sistemi di storage NetApp e Celerra, il modello di dati Chargeback utilizza un singolo livello (di volumi, volumi interni o qtree) per basare i propri addebiti, mentre il modello di dati Storage Capacity utilizza più livelli (di volumi e volumi interni) per basare i propri addebiti.

Modello di dati di inventario

Consente di rispondere a domande sulle risorse di inventario, tra cui host, sistemi di archiviazione, switch, dischi, nastri, qtree, quote, macchine virtuali e server e dispositivi generici. Il modello di dati Inventory include diversi sottomart che consentono di visualizzare informazioni su repliche, percorsi FC, percorsi iSCSI, percorsi NFS e violazioni. Il modello di dati di inventario non include dati storici. Domande a cui puoi rispondere con questi dati

- Quali beni ho e dove sono?
- Chi utilizza le risorse?
- Che tipo di dispositivi ho e quali sono i componenti di tali dispositivi?
- Quanti host ho per sistema operativo e quante porte ci sono su quegli host?
- Quali array di storage per fornitore sono presenti in ciascun data center?
- Quanti switch per fornitore ho in ogni data center?

- Quanti porti non sono autorizzati?
- Quali nastri del fornitore stiamo utilizzando e quante porte sono presenti su ciascun nastro? Sono stati identificati tutti i dispositivi generici prima di iniziare a lavorare sui report?
- Quali sono i percorsi tra host e volumi di archiviazione o nastri?
- Quali sono i percorsi tra dispositivi generici e volumi di archiviazione o nastri?
- Quante violazioni di ogni tipo ho per data center?
- Per ogni volume replicato, quali sono i volumi di origine e di destinazione?
- Ci sono incompatibilità di firmware o discrepanze di velocità delle porte tra gli HBA host Fibre Channel e gli switch?

Modello di dati sulle prestazioni

Consente di rispondere a domande sulle prestazioni di volumi, volumi applicativi, volumi interni, switch, applicazioni, VM, VMDK, ESX rispetto a VM, host e nodi applicativi. Molti di questi riportano dati *orari*, dati *giornalieri* o entrambi. Utilizzando questo modello di dati, è possibile creare report che rispondono a diversi tipi di domande sulla gestione delle prestazioni:

- Quali volumi o volumi interni non sono stati utilizzati o consultati durante un periodo specifico?
- Possiamo individuare eventuali errori di configurazione per l'archiviazione di un'applicazione (non utilizzata)?
- Qual era il modello generale di comportamento di accesso per un'applicazione?
- I volumi a livelli sono assegnati in modo appropriato per una determinata applicazione?
- Potremmo utilizzare uno spazio di archiviazione più economico per un'applicazione attualmente in esecuzione senza compromettere le prestazioni dell'applicazione?
- Quali sono le applicazioni che generano più accessi allo storage attualmente configurato?

Utilizzando le tabelle delle prestazioni dello switch, è possibile ottenere le seguenti informazioni:

- Il traffico del mio host attraverso le porte connesse è bilanciato?
- Quali switch o porte presentano un numero elevato di errori?
- Quali sono gli switch più utilizzati in base alle prestazioni delle porte?
- Quali sono gli switch sottoutilizzati in base alle prestazioni delle porte?
- Qual è l'andamento della produttività dell'host in base alle prestazioni della porta?
- Qual è stato l'utilizzo delle prestazioni negli ultimi X giorni per un host, un sistema di archiviazione, un nastro o uno switch specificato?
- Quali dispositivi producono traffico su uno switch specifico (ad esempio, quali dispositivi sono responsabili dell'utilizzo di uno switch molto utilizzato)?
- Qual è la produttività di una specifica unità aziendale nel nostro ambiente?

Utilizzando le tabelle delle prestazioni del disco, è possibile ottenere le seguenti informazioni:

- Qual è la produttività per un pool di archiviazione specificato in base ai dati sulle prestazioni del disco?
- Qual è il pool di archiviazione più utilizzato?
- Qual è l'utilizzo medio del disco per uno specifico storage?
- Qual è la tendenza di utilizzo di un sistema di archiviazione o di un pool di archiviazione in base ai dati

sulle prestazioni del disco?

- Qual è l'andamento dell'utilizzo del disco per uno specifico pool di archiviazione?

Quando si utilizzano le tabelle delle prestazioni VM e VMDK, è possibile ottenere le seguenti informazioni:

- Il mio ambiente virtuale funziona in modo ottimale?
- Quali VMDK segnalano i carichi di lavoro più elevati?
- Come posso utilizzare le prestazioni segnalate dai VMD mappati su diversi datastore per prendere decisioni sulla riorganizzazione in livelli?

Il modello di dati Performance include informazioni che aiutano a determinare l'adeguatezza dei livelli, le configurazioni errate di archiviazione per le applicazioni e gli orari dell'ultimo accesso dei volumi e dei volumi interni. Questo modello di dati fornisce dati quali tempi di risposta, IOPS, throughput, numero di scritture in sospeso e stato di accesso.

Modello di dati di efficienza di archiviazione

Consente di monitorare il punteggio e il potenziale di efficienza dello storage nel tempo. Questo modello di dati memorizza le misurazioni non solo della capacità fornita, ma anche della quantità utilizzata o consumata (la misurazione fisica). Ad esempio, quando è abilitato il thin provisioning, Data Infrastructure Insights indica quanta capacità viene utilizzata dal dispositivo. È possibile utilizzare questo modello anche per determinare l'efficienza quando la deduplicazione è abilitata. Utilizzando il data mart Storage Efficiency è possibile rispondere a diverse domande:

- Quali sono i risparmi in termini di efficienza di storage ottenuti grazie all'implementazione di tecnologie di thin provisioning e deduplicazione?
- Quali sono i risparmi di spazio di archiviazione nei data center?
- In base ai trend storici della capacità, quando è necessario acquistare ulteriore spazio di archiviazione?
- Quale sarebbe il guadagno di capacità se abilitassimo tecnologie come il thin provisioning e la deduplicazione?
- Per quanto riguarda la capacità di archiviazione, sono a rischio adesso?

Tabelle dei fatti e delle dimensioni del modello di dati

Ogni modello di dati include sia tabelle dei fatti che tabelle delle dimensioni.

- Tabelle dei fatti: contengono dati misurati, ad esempio quantità, capacità grezza e utilizzabile. Contiene chiavi esterne per le tabelle delle dimensioni.
- Tabelle dimensionali: contengono informazioni descrittive sui fatti, ad esempio data center e unità aziendali. Una dimensione è una struttura, spesso composta da gerarchie, che categorizza i dati. Gli attributi dimensionali aiutano a descrivere i valori dimensionali.

Utilizzando attributi di dimensione diversi o multipli (visualizzati come colonne nei report), è possibile creare report che accedono ai dati per ciascuna dimensione descritta nel modello di dati.

Colori utilizzati negli elementi del modello dati

I colori sugli elementi del modello dati hanno indicazioni diverse.

- Risorse gialle: rappresentano le misurazioni.
- Risorse non gialle: rappresentano attributi. Questi valori non si sommano.

Utilizzo di più modelli di dati in un unico report

In genere, si utilizza un modello di dati per report. Tuttavia, è possibile scrivere un report che combini dati provenienti da più modelli di dati.

Per scrivere un report che combina dati provenienti da più modelli di dati, scegli uno dei modelli di dati da utilizzare come base, quindi scrivi query SQL per accedere ai dati dai data mart aggiuntivi. È possibile utilizzare la funzionalità SQL Join per combinare i dati provenienti da diverse query in un'unica query che è possibile utilizzare per scrivere il report.

Ad esempio, supponiamo di voler conoscere la capacità corrente di ogni array di archiviazione e di voler acquisire annotazioni personalizzate sugli array. È possibile creare il report utilizzando il modello di dati Capacità di archiviazione. È possibile utilizzare gli elementi delle tabelle Capacità corrente e Dimensioni e aggiungere una query SQL separata per accedere alle informazioni sulle annotazioni nel modello di dati Inventario. Infine, è possibile combinare i dati collegando i dati di archiviazione dell'inventario alla tabella delle dimensioni di archiviazione utilizzando il nome dell'archiviazione e i criteri di unione.

Accedi al database di reporting tramite API

La potente API di Data Infrastructure Insights consente agli utenti di interrogare direttamente il database di reporting di Data Infrastructure Insights , senza passare attraverso l'ambiente di reporting di Cognos.

Questa documentazione fa riferimento alla funzionalità di reporting di Data Infrastructure Insights , disponibile in Data Infrastructure Insights Premium Edition.

Odata

L'API di reporting di Data Infrastructure Insights segue"OData v4" (Open Data Protocol) standard per l'interrogazione del database di reporting. Per maggiori informazioni o per saperne di più, consulta"questo tutorial" su OData.

Tutte le richieste inizieranno con l'URL *https://< URL Data Infrastructure Insights >/rest/v1/dwh-management/odata*

Generazione di una APIKey

Per saperne di più"API Data Infrastructure Insights" .

Per generare una chiave API, procedere come segue:

- Accedi al tuo ambiente Data Infrastructure Insights e seleziona **Amministrazione > Accesso API**.
- Fare clic su "+ Token di accesso API".
- Inserisci un nome e una descrizione.
- Per il tipo, seleziona *Data Warehouse*.
- Imposta i permessi come Lettura/Scrittura.
- Imposta una data di scadenza per i desideri.
- Fai clic su "Salva", quindi **copia la chiave e salvala** in un luogo sicuro. In seguito non sarà più possibile accedere alla chiave completa.

Le chiavi API sono utili per*Sincronizzazione* o *Asincrono* .

Interrogazione diretta delle tabelle

Con la chiave API in atto, ora è possibile effettuare query dirette al database di reporting. Gli URL lunghi possono essere semplificati in https://…/odata/ per scopi di visualizzazione anziché nel formato completo https://< URL Data Infrastructure Insights >/rest/v1/dwh-management/odata/

Prova semplici query come

- https://< URL di Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_custom
- https://< URL di Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory
- https://< URL di Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/storage
- https://< URL di Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/disk
- https://…/odata/dwh_custom/custom_queries

Esempi di API REST

L'URL per tutte le chiamate è *https://< URL Data Infrastructure Insights >/rest/v1/dwh-management/odata*.

- GET /{schema}/** - Recupera i dati dal database di reporting.

Formato: *https://< URL Data Infrastructure Insights >/rest/v1/dwh-management/odata/<nome_schema>/<query>*

Esempio:

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
Risultato:
```

```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```


Suggerimenti utili

Quando si utilizzano le query dell'API di reporting, tenere presente quanto segue.

- Il payload della query deve essere una stringa JSON valida
- Il payload della query deve essere contenuto in una singola riga
- Le virgolette doppie devono essere precedute da escape, ad esempio \"
- Le schede sono supportate come \t
- Evita i commenti
- Sono supportati i nomi delle tabelle in minuscolo

Inoltre:

- Sono richieste 2 intestazioni:
  - Nome "X-CloudInsights-ApiKey"
  - Valore attributo "<apikey>"

La tua chiave API sarà specifica per il tuo ambiente Data Infrastructure Insights .

Sincrono o asincrono?

Per impostazione predefinita, un comando API funziona in modalità *sincrona*, ovvero quando si invia la richiesta, la risposta viene restituita immediatamente. Tuttavia, a volte l'esecuzione di una query potrebbe richiedere molto tempo, il che potrebbe causare il timeout della richiesta. Per aggirare questo problema, è possibile eseguire una richiesta in modo *asincrono*. In modalità asincrona, la richiesta restituirà un URL tramite il quale è possibile monitorare l'esecuzione. L'URL restituirà il risultato quando sarà pronto.

Per eseguire una query in modalità asincrona, aggiungere l'intestazione **`Prefer: respond-async`** alla richiesta. In caso di esecuzione corretta, la risposta conterrà le seguenti intestazioni:

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

L'interrogazione dell'URL della posizione restituirà le stesse intestazioni se la risposta non è ancora pronta oppure restituirà lo stato 200 se la risposta è pronta. Il contenuto della risposta sarà di tipo testo e conterrà lo stato http della query originale e alcuni metadati, seguiti dai risultati della query originale.

```
HTTP/1.1 200 OK
 OData-Version: 4.0
 Content-Type: application/json;odata.metadata=minimal
 oDataResponseSizeCounted: true

 { <JSON_RESPONSE> }
```

Per visualizzare un elenco di tutte le query asincrone e quali di esse sono pronte, utilizzare il seguente comando:

```
 GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
La risposta ha il seguente formato:
```

```
{
   "queries" : [
       {
           "Query": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
           "Location": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-management/odata/dwh_custom/asyncStatus/<token>",
           "Finished": false
       }
   ]
}
```

Pubblicazione e annullamento della pubblicazione di annotazioni per la segnalazione

Pubblicazione e annullamento della pubblicazione di annotazioni per la segnalazione

Scopri come pubblicare annotazioni da utilizzare nei report e nel Data Warehouse e come annullare correttamente la pubblicazione delle annotazioni quando non sono più necessarie.

Pubblicazione di annotazioni per la segnalazione

Dopo aver creato annotazioni in Data Infrastructure Insights, puoi pubblicarle per utilizzarle in Reporting.

Passaggi per pubblicare annotazioni

1. Vai alla pagina *Osservabilità > Arricchisci > Annotazioni e seleziona la scheda *Annotazioni per la creazione di report*.
2. Individua l'annotazione che desideri pubblicare.
3. Selezionare l'annotazione e selezionare *Pubblica nei report*. È anche possibile scegliere di applicarlo ai dati storici, consentendo di utilizzare l'annotazione durante l'esecuzione di report cronologici.
4. Una volta pubblicata, l'annotazione diventa disponibile per l'uso in Reporting.
5. Le annotazioni vengono pubblicate per essere utilizzate nella creazione di report dopo la successiva esecuzione ETL.

> Tutti i report che fanno riferimento all'annotazione utilizzeranno i valori pubblicati. Se modifichi un'annotazione dopo la pubblicazione, potrebbe essere necessario ripubblicarla affinché le modifiche abbiano effetto nei report.

Annullamento della pubblicazione delle annotazioni per la segnalazione

Potrebbero esserci momenti in cui è necessario rimuovere o annullare la pubblicazione delle annotazioni, in modo che non vengano più utilizzate in Reporting. Ad esempio, un'annotazione potrebbe non essere più necessaria oppure potrebbe contenere informazioni obsolete che non dovrebbero comparire nei report.

Passaggi per annullare la pubblicazione delle annotazioni

Prima di annullare la pubblicazione di un'annotazione, tieni presente che questa azione avrà un impatto su tutti i report esistenti che utilizzano l'annotazione. I report potrebbero richiedere la modifica o l'assistenza di servizi professionali per rimuovere i riferimenti alle annotazioni.

1. Nell'interfaccia utente Data Infrastructure Insights , vai alla scheda *Annotazioni per la creazione di report*.
2. Individua l'annotazione di cui vuoi annullare la pubblicazione.
3. Per ogni oggetto in cui è pubblicata l'annotazione, deselezionare l'annotazione e selezionare *Salva*.
4. Rimuovere tutte le query o le regole che fanno ancora riferimento all'annotazione per assicurarsi che non venga contrassegnata come "in uso".
5. Le annotazioni non saranno pubblicate dopo la successiva esecuzione ETL.
6. Una volta completato l'ETL, l'annotazione può essere eliminata dall'elenco delle annotazioni, se non è più necessaria sul lato tenant.

> Le annotazioni continueranno ad apparire nel Data Warehouse finché non verranno opportunamente rimosse dalla pubblicazione. La semplice eliminazione di un'annotazione dalla pagina Annotazioni senza prima annullarne la pubblicazione lascerà dati obsoleti che potrebbero apparire nei report esistenti. Per garantire la rimozione completa, seguire i passaggi di annullamento della pubblicazione indicati sopra.

Impatto sui report esistenti

La rimozione o l'annullamento della pubblicazione delle annotazioni potrebbe richiedere modifiche ai report esistenti che fanno riferimento a tali annotazioni. Considera quanto segue:

- I report che utilizzano l'annotazione come filtro o dimensione dovranno essere aggiornati.
- Se un'annotazione viene rimossa senza aggiornare i report dipendenti, tali report potrebbero restituire errori o risultati imprevisti.
- Potrebbe essere necessario ricorrere a servizi professionali per assistere nella correzione dei report in scenari complessi.

Si consiglia di rivedere tutti i report che dipendono da un'annotazione prima di annullarne la pubblicazione.

Come vengono conservati i dati storici per la creazione di report

Data Infrastructure Insights conserva i dati storici da utilizzare nei report in base ai data mart e alla granularità dei dati, come mostrato nella tabella seguente.

Data mart	Oggetto misurato	Granularità	Periodo di conservazione
Mercati delle prestazioni	Volumi e volumi interni	Ogni ora	14 giorni
Mercati delle prestazioni	Volumi e volumi interni	Quotidiano	13 mesi
Mercati delle prestazioni	Applicazione	Ogni ora	13 mesi
Mercati delle prestazioni	Ospite	Ogni ora	13 mesi
Mercati delle prestazioni	Prestazioni dello switch per porta	Ogni ora	35 giorni

Mercati delle prestazioni	Cambia le prestazioni per host, storage e nastro	Ogni ora	13 mesi
Mercati delle prestazioni	Nodo di archiviazione	Ogni ora	14 giorni
Mercati delle prestazioni	Nodo di archiviazione	Quotidiano	13 mesi
Mercati delle prestazioni	Prestazioni della VM	Ogni ora	14 giorni
Mercati delle prestazioni	Prestazioni della VM	Quotidiano	13 mesi
Mercati delle prestazioni	Prestazioni dell'hypervisor	Ogni ora	35 giorni
Mercati delle prestazioni	Prestazioni dell'hypervisor	Quotidiano	13 mesi
Mercati delle prestazioni	Prestazioni della VMDK	Ogni ora	35 giorni
Mercati delle prestazioni	Prestazioni della VMDK	Quotidiano	13 mesi
Mercati delle prestazioni	Prestazioni del disco	Ogni ora	14 giorni
Mercati delle prestazioni	Prestazioni del disco	Quotidiano	13 mesi
Mercati di capacità	Tutti (tranne i singoli volumi)	Quotidiano	13 mesi
Mercati di capacità	Tutti (tranne i singoli volumi)	Rappresentante mensile	14 mesi e oltre
Mercati di inventario	Volumi individuali	Stato attuale	1 giorno (o fino al prossimo ETL)

Diagrammi di schema di reporting Data Infrastructure Insights

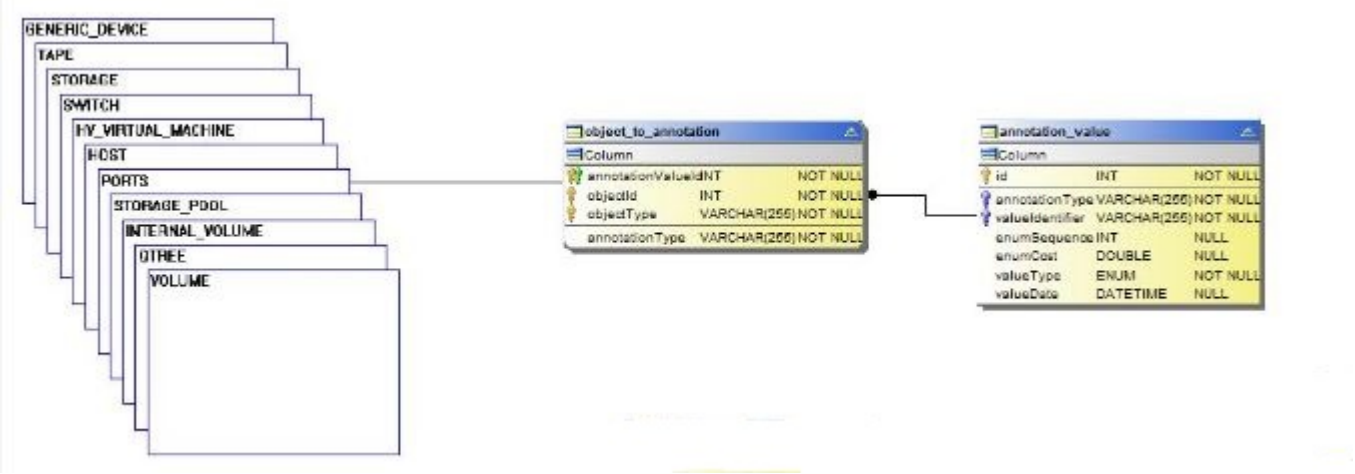
Questo documento fornisce diagrammi di schema per il database di reporting.

La funzionalità di reporting è disponibile in Data Infrastructure Insights"Edizione Premium" .

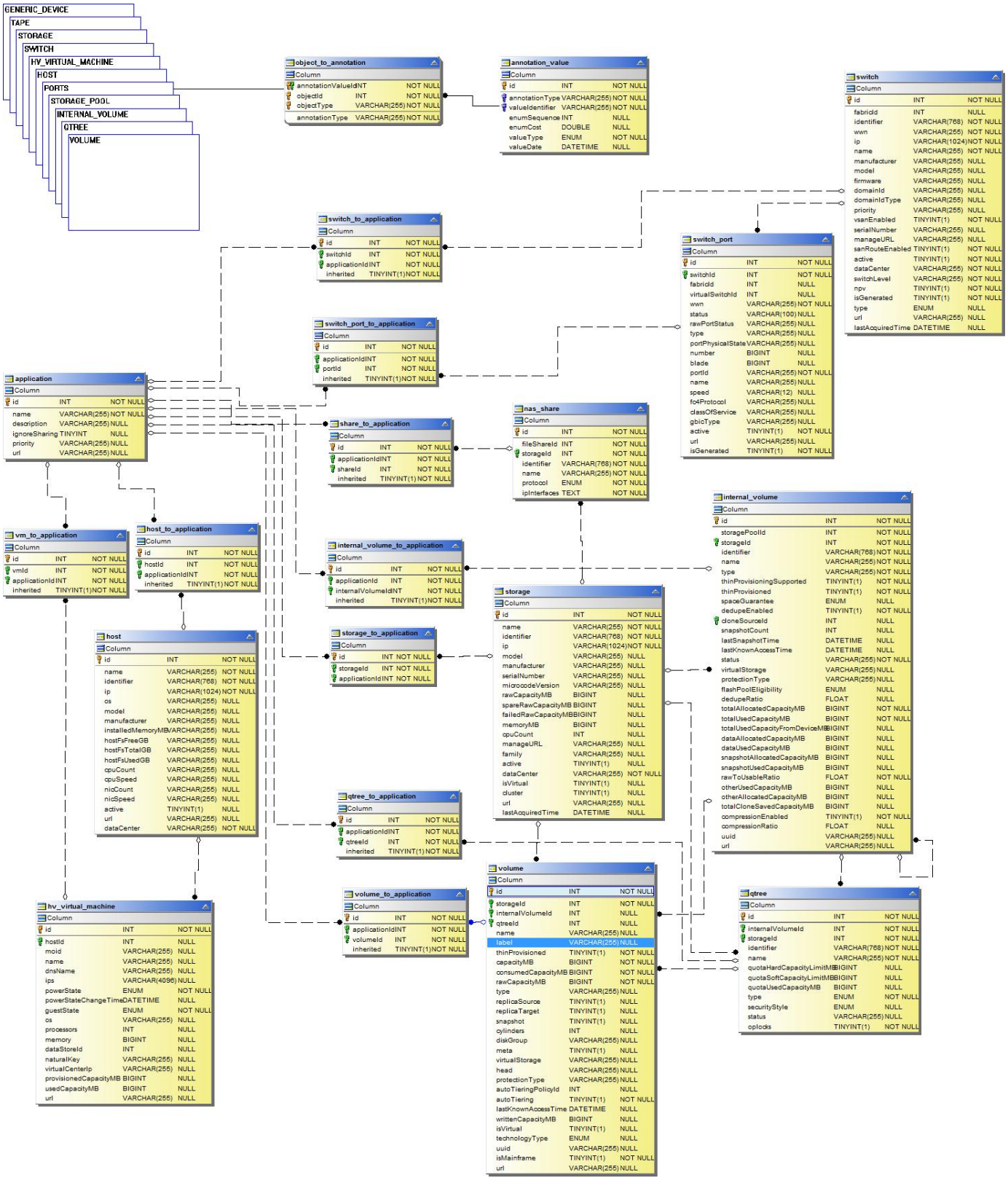
Datamart di inventario

Le immagini seguenti descrivono il datamart dell'inventario.

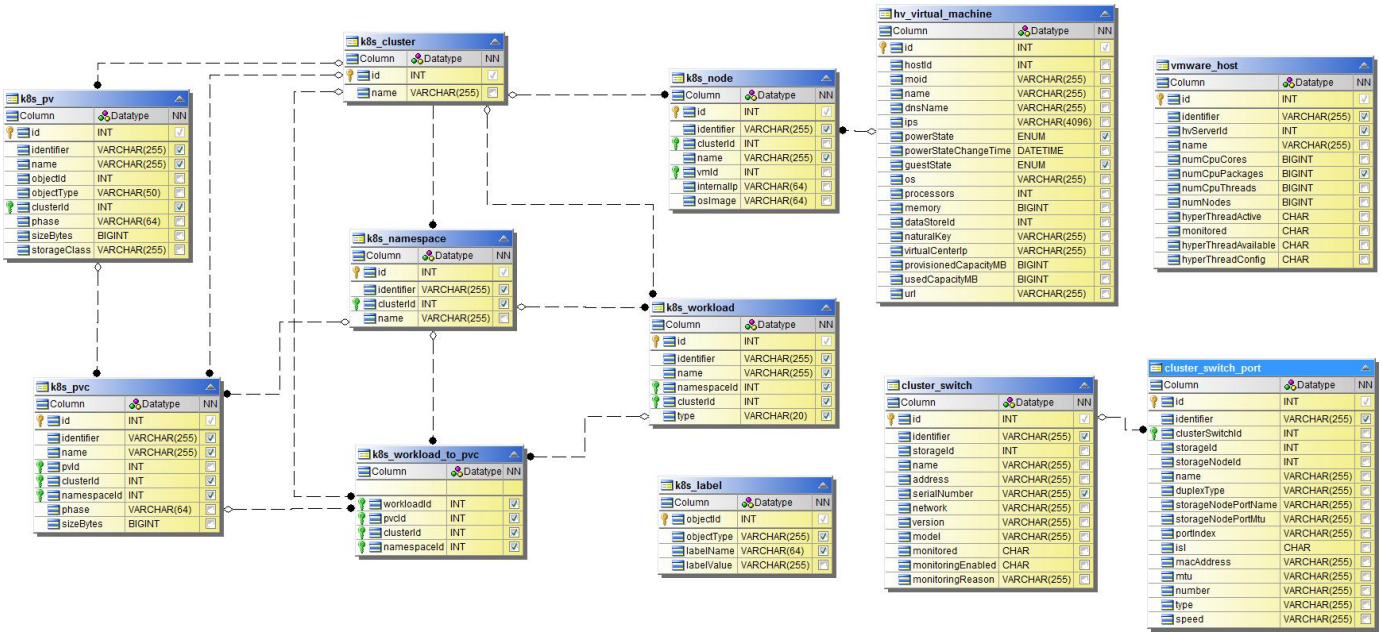
Annotazioni



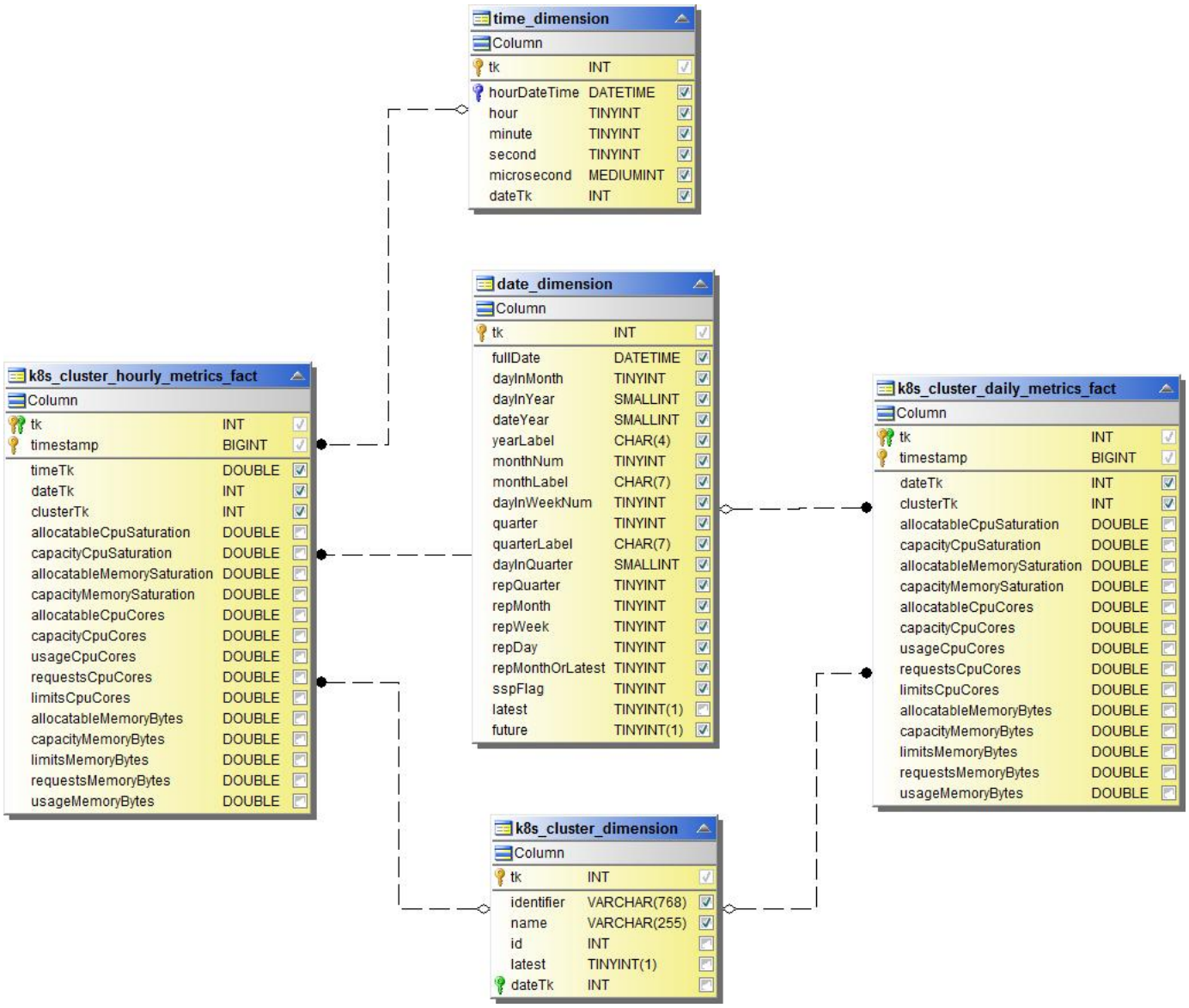
Applicazioni



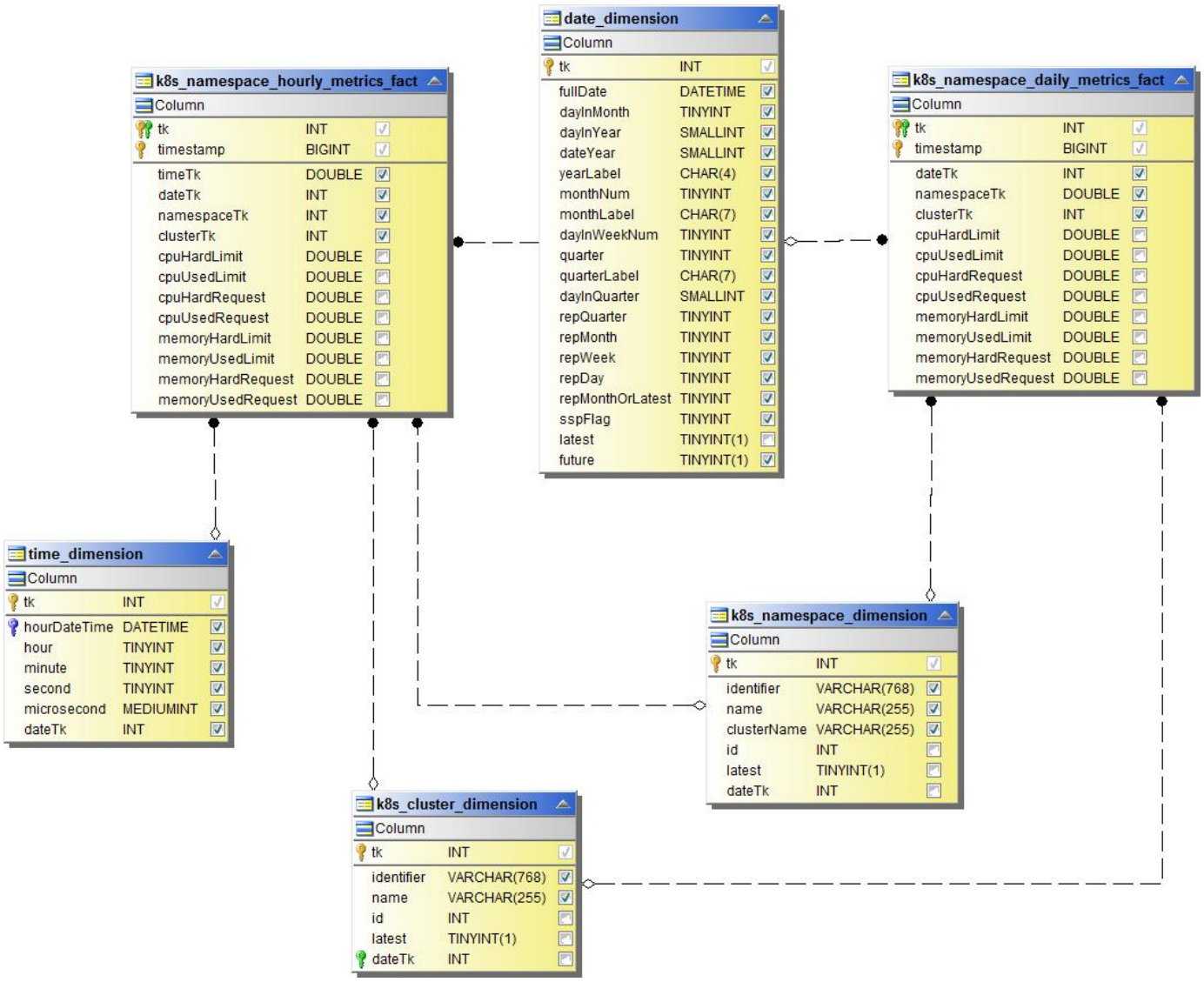
Metriche di Kubernetes



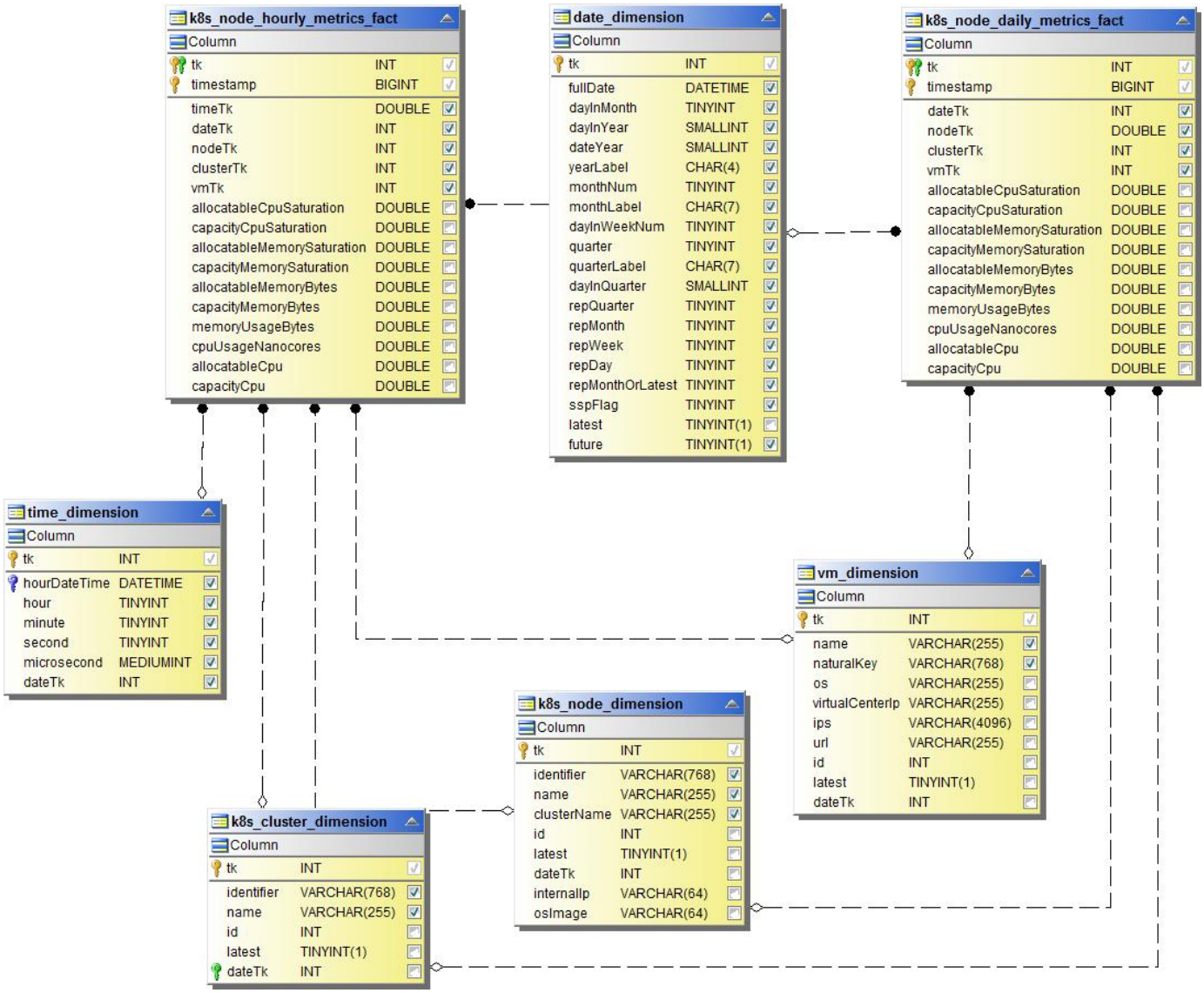
Fatto sulle metriche del cluster Kubernetes



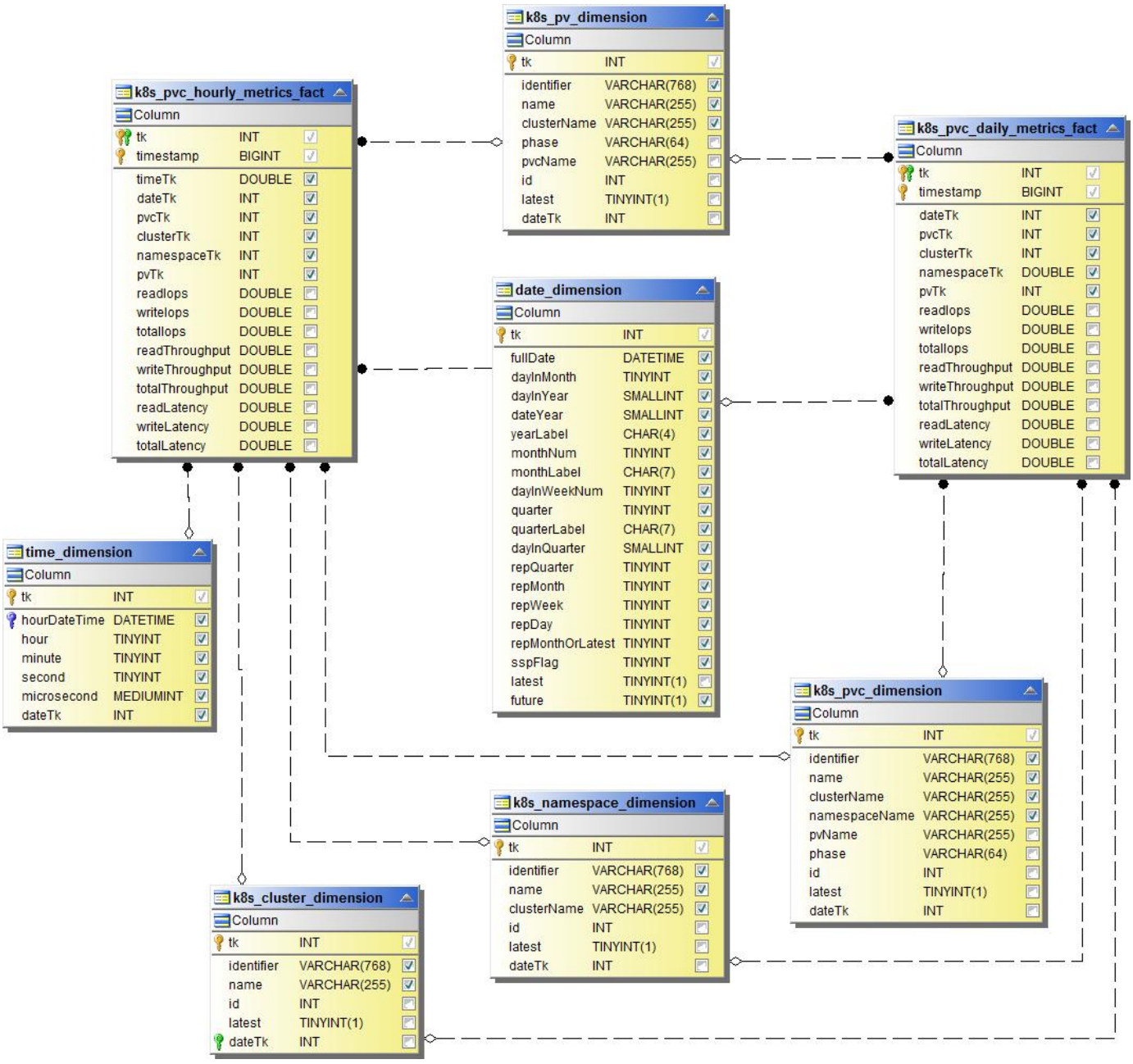
Fatto sulle metriche dello spazio dei nomi di Kubernetes



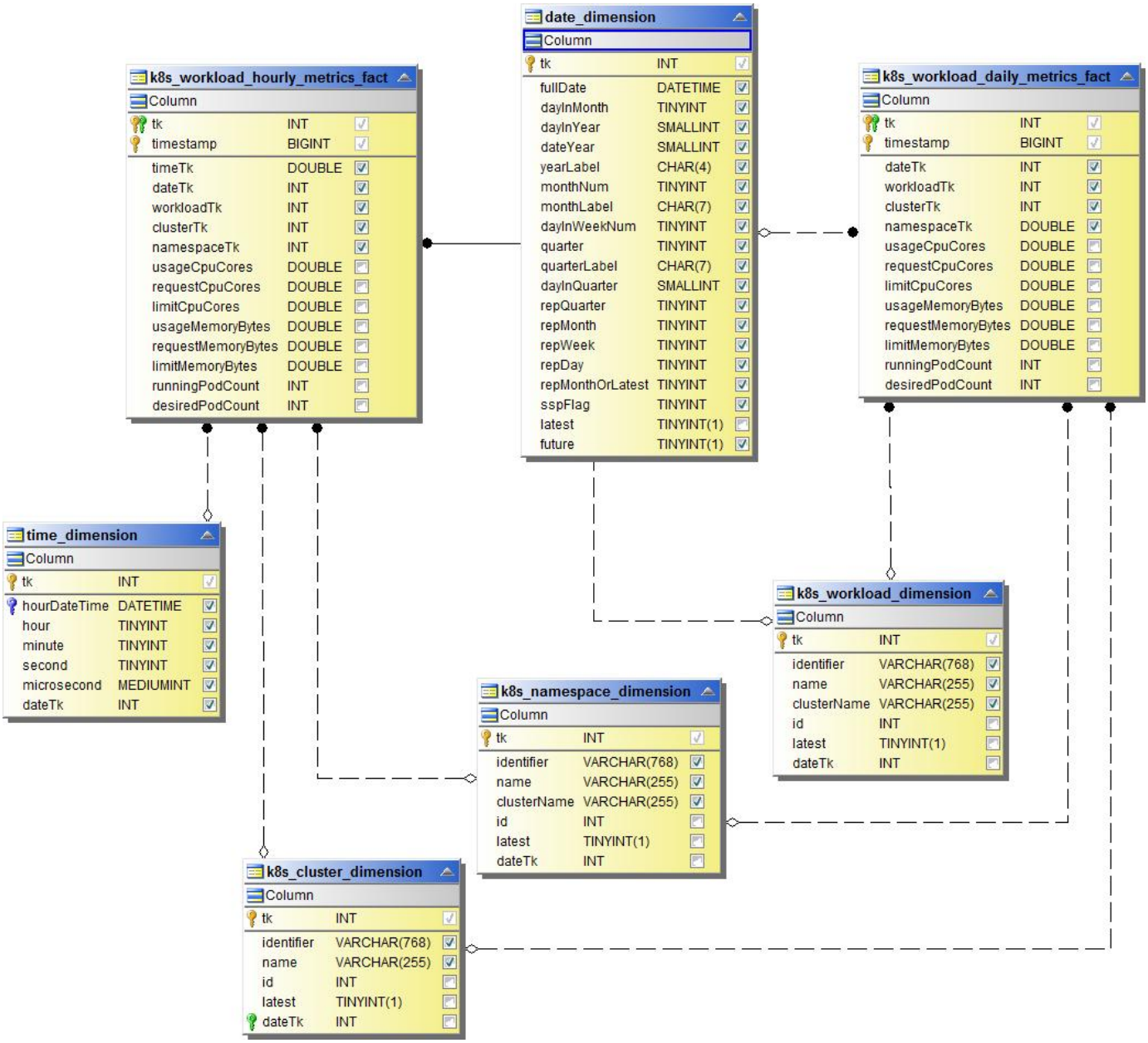
Fatto sulle metriche dei nodi Kubernetes



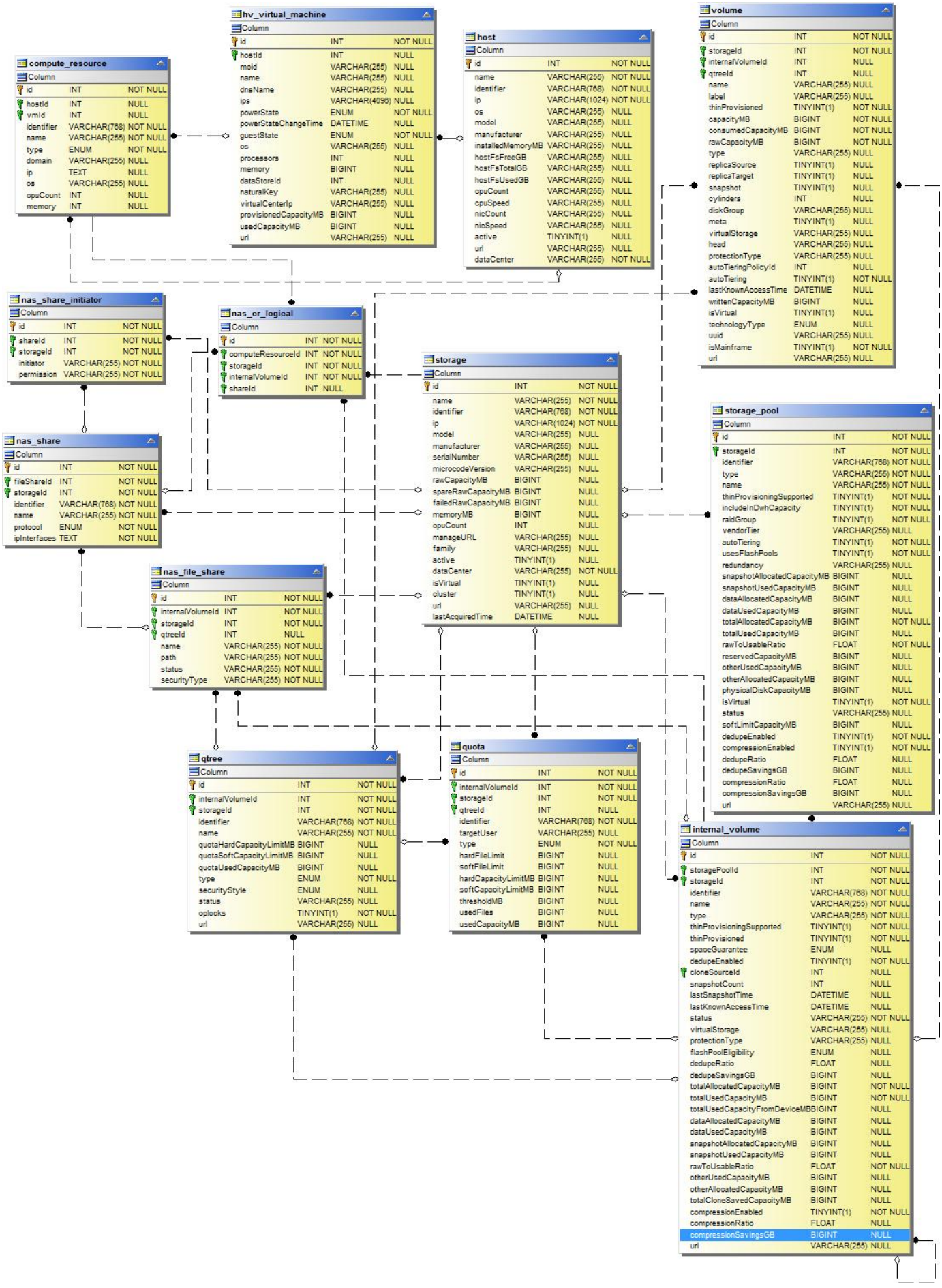
Fatto sulle metriche PVC di Kubernetes



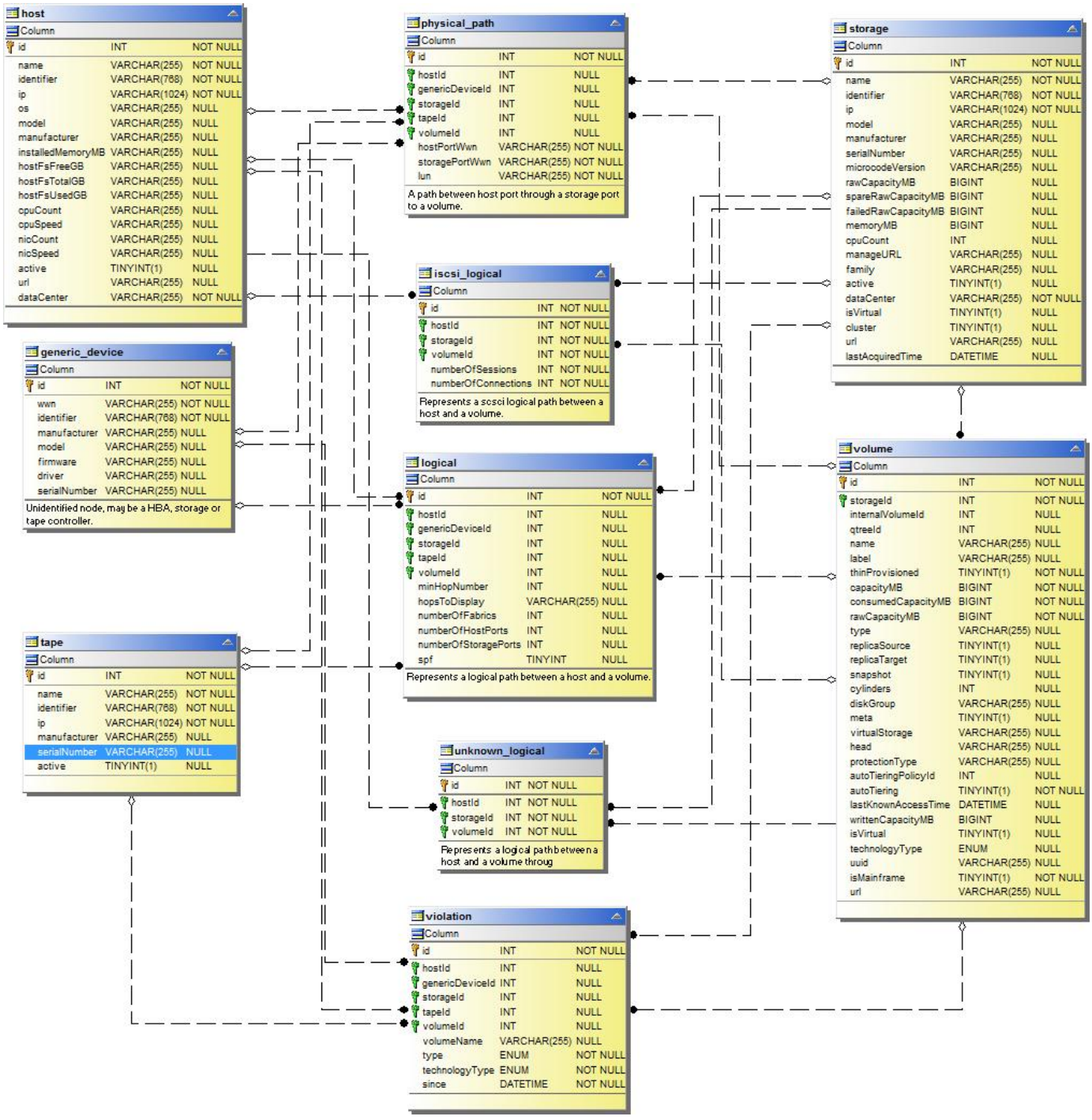
Fatto sulle metriche del carico di lavoro di Kubernetes


date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

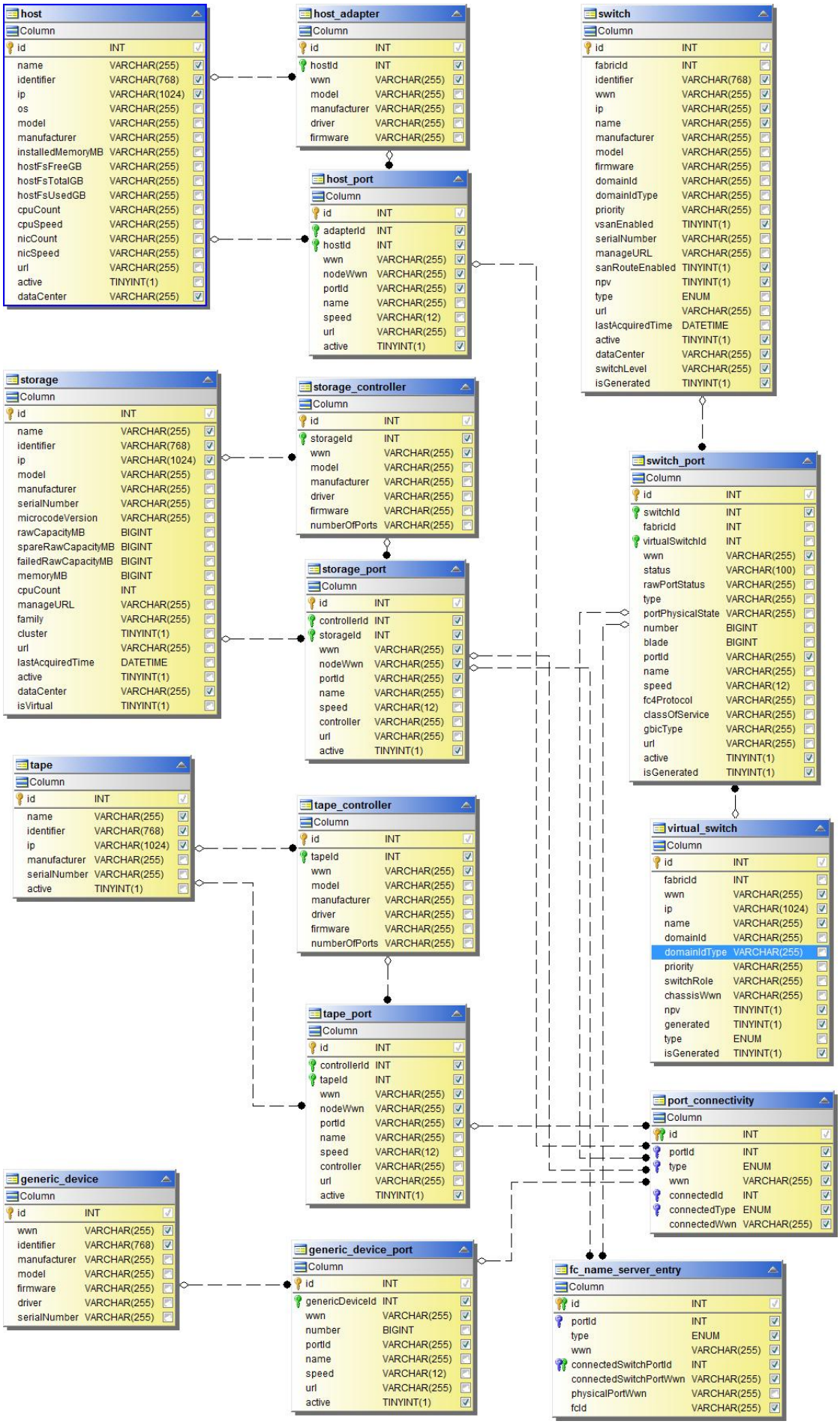
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDwhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL

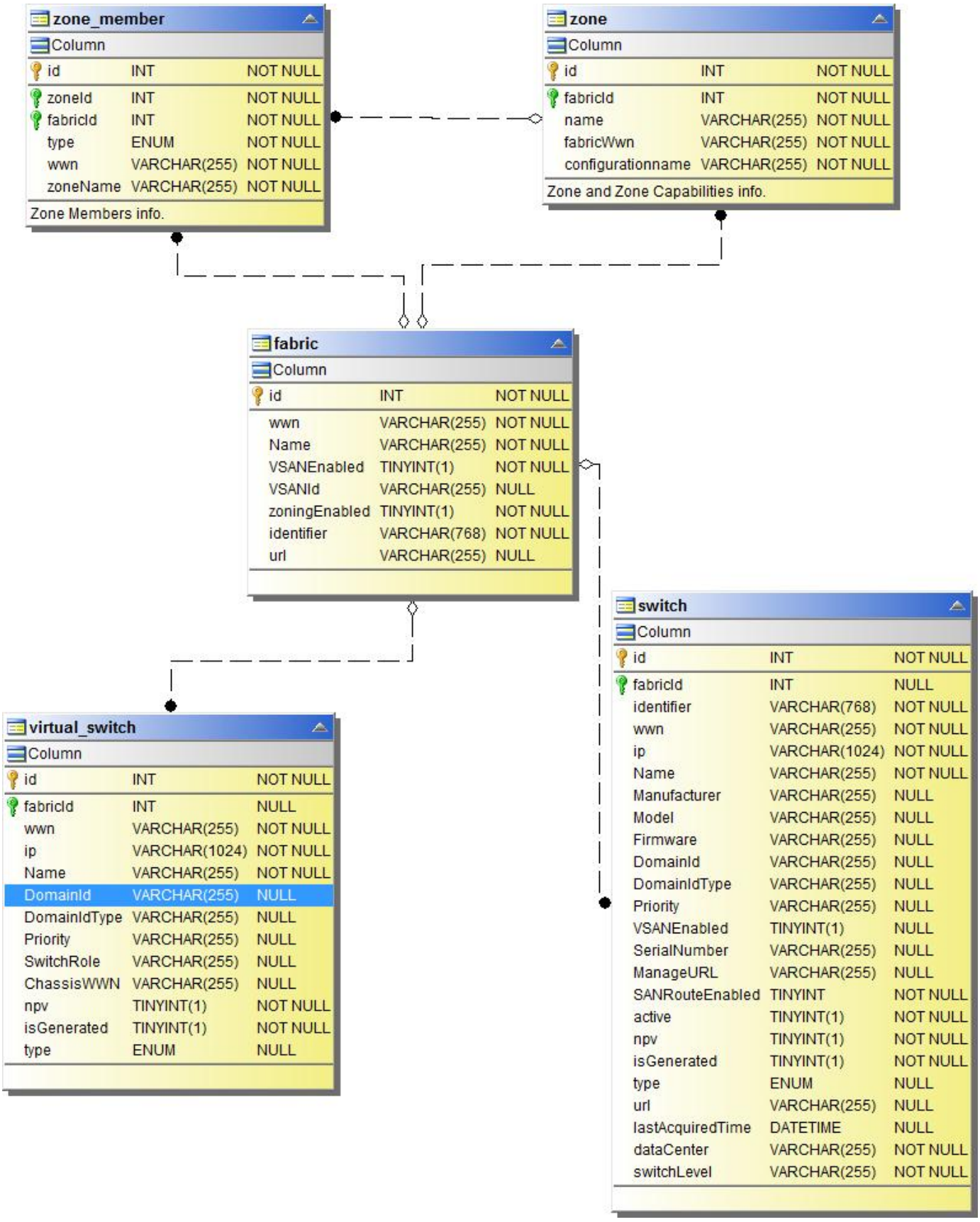
Percorsi e violazioni



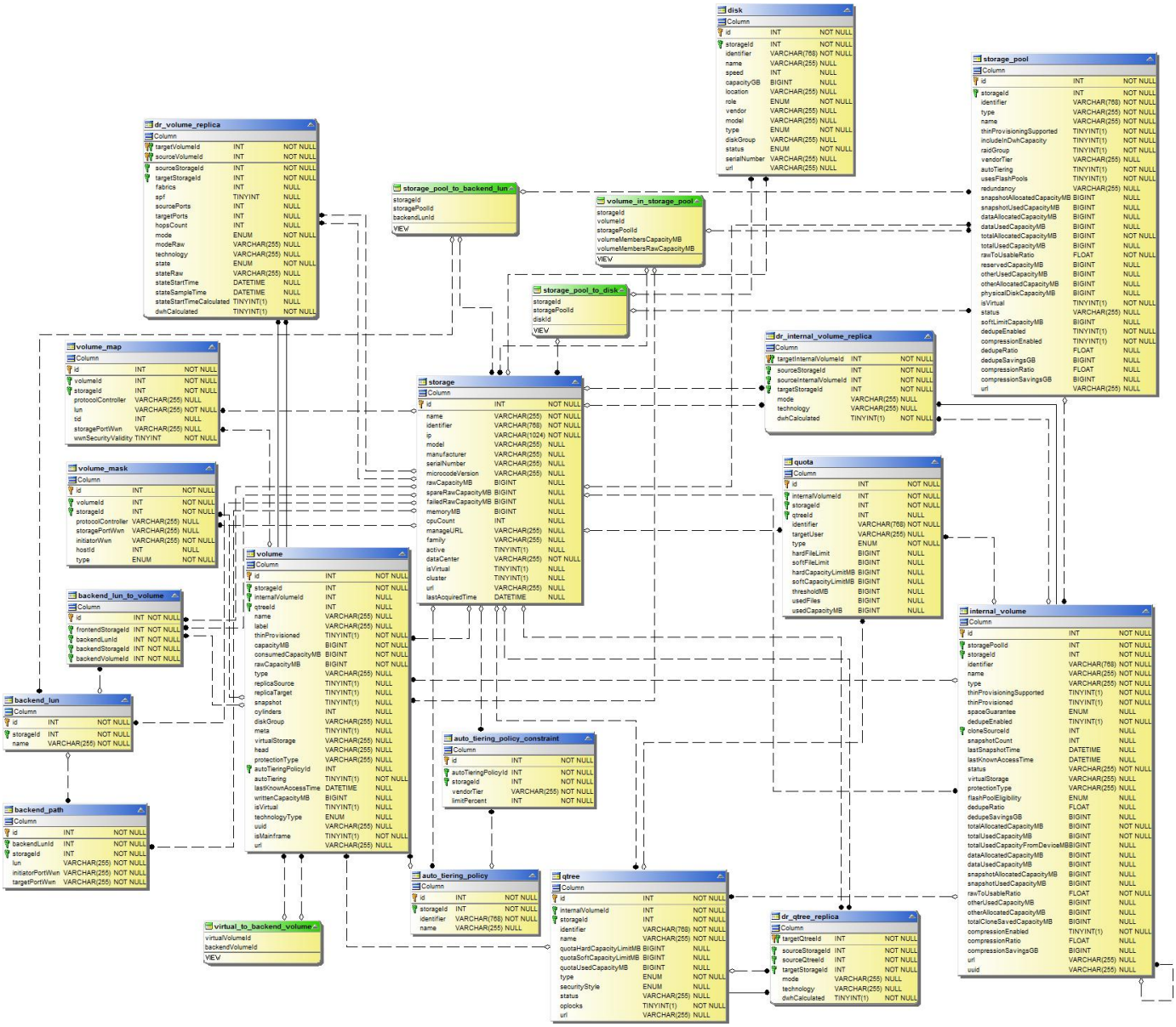
Connettività delle porte


host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(1024)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

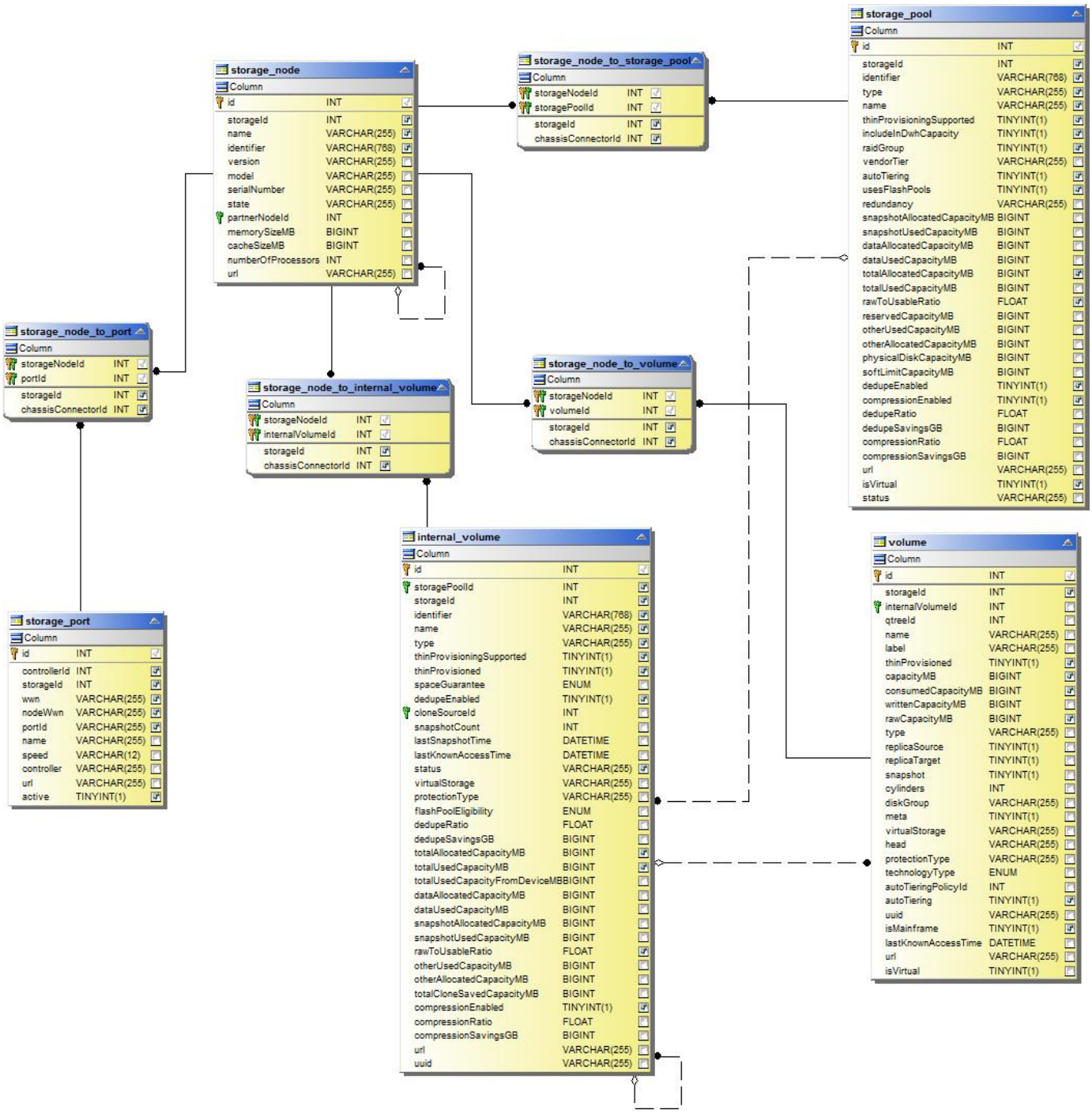
Tessuto SAN


zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL

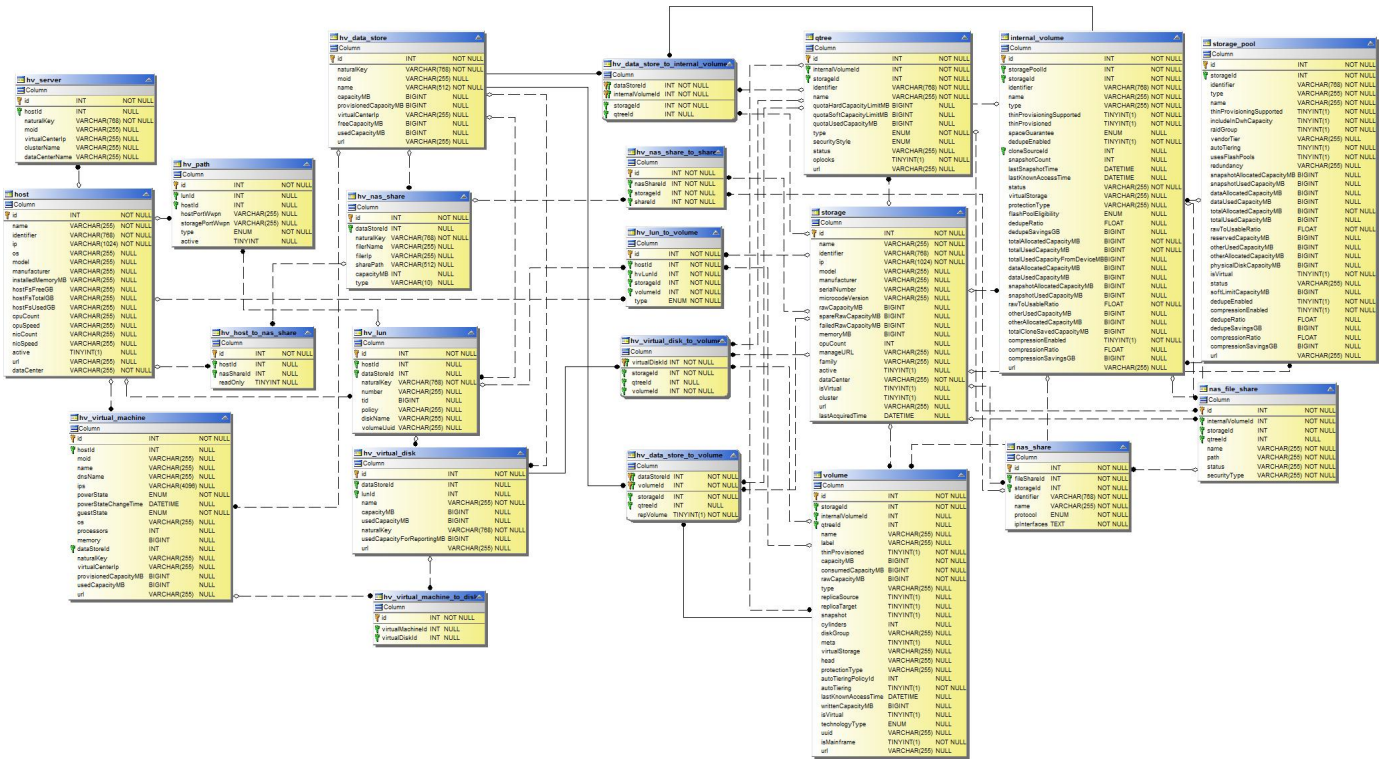
Magazzinaggio



Nodo di archiviazione



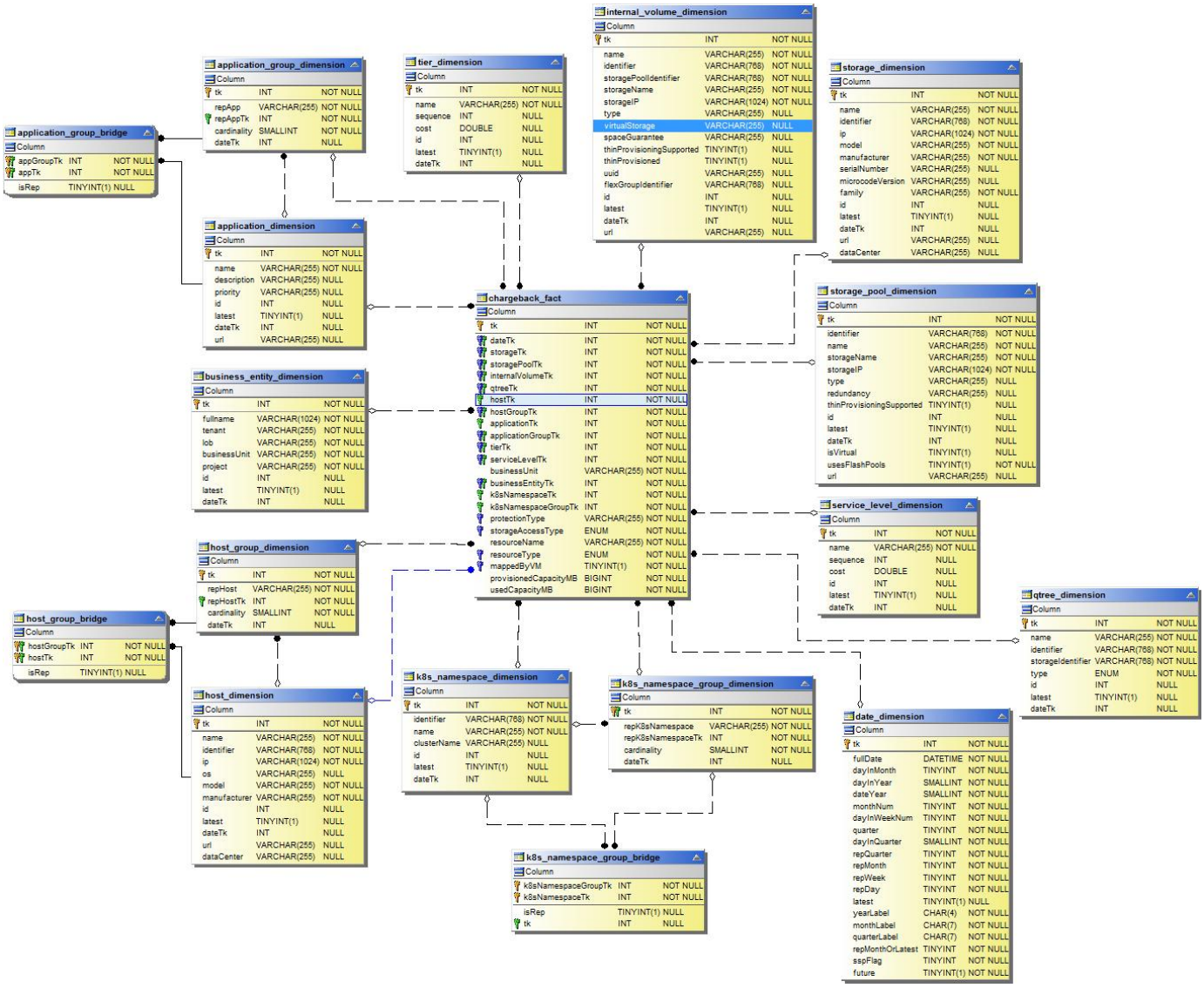
Macchina virtuale



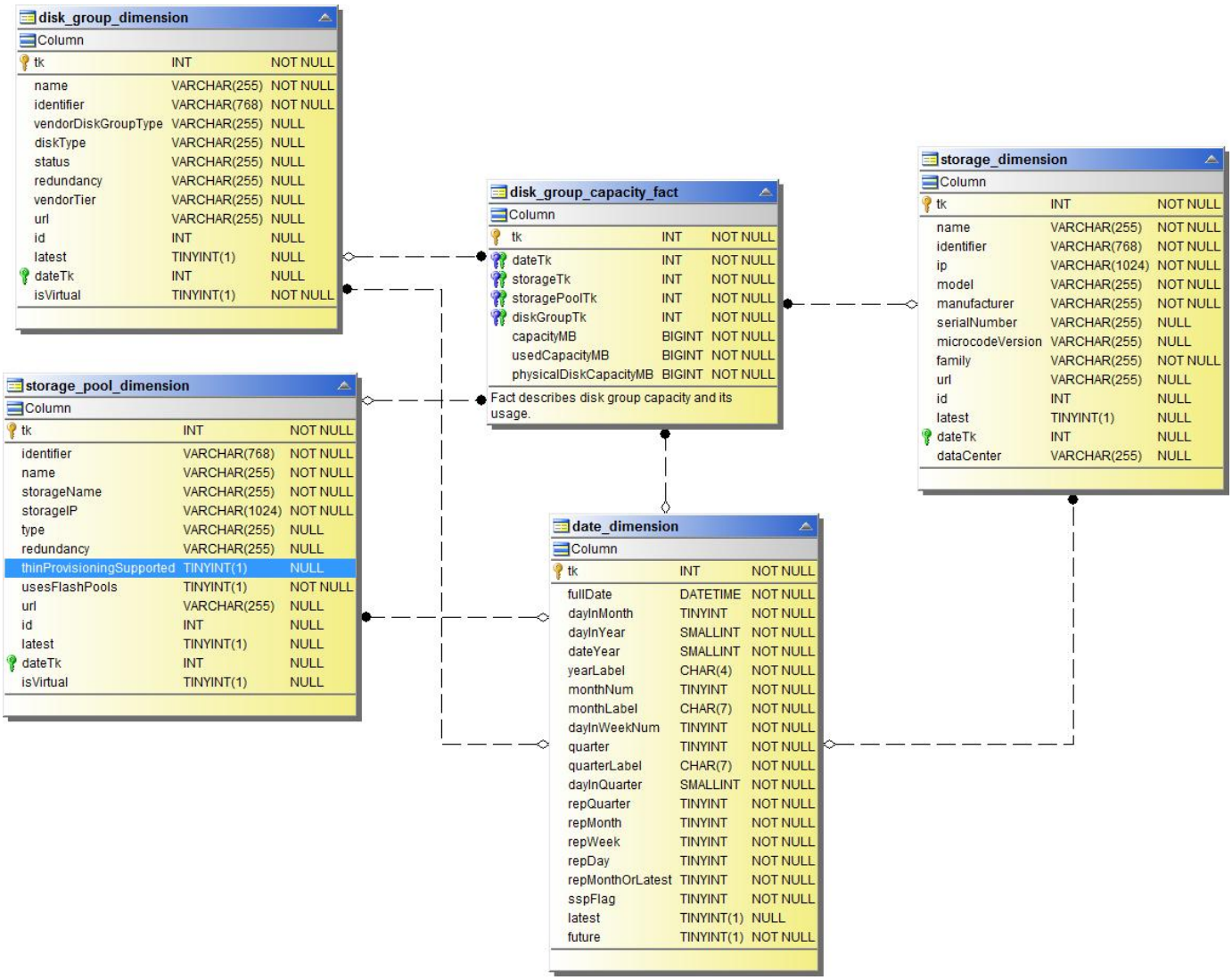
Datamart di capacità

Le immagini seguenti descrivono il datamart della capacità.

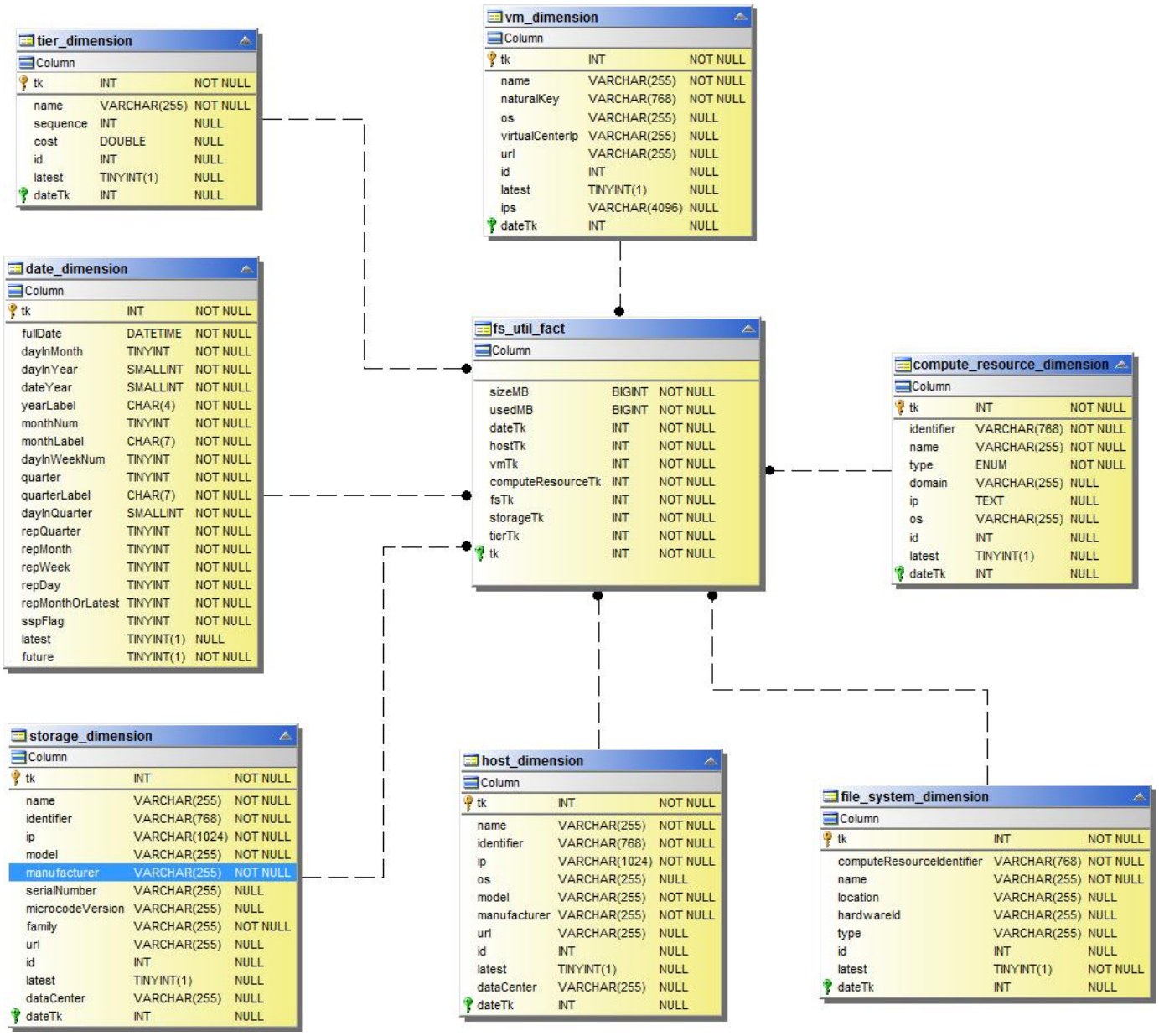
Riaddebito



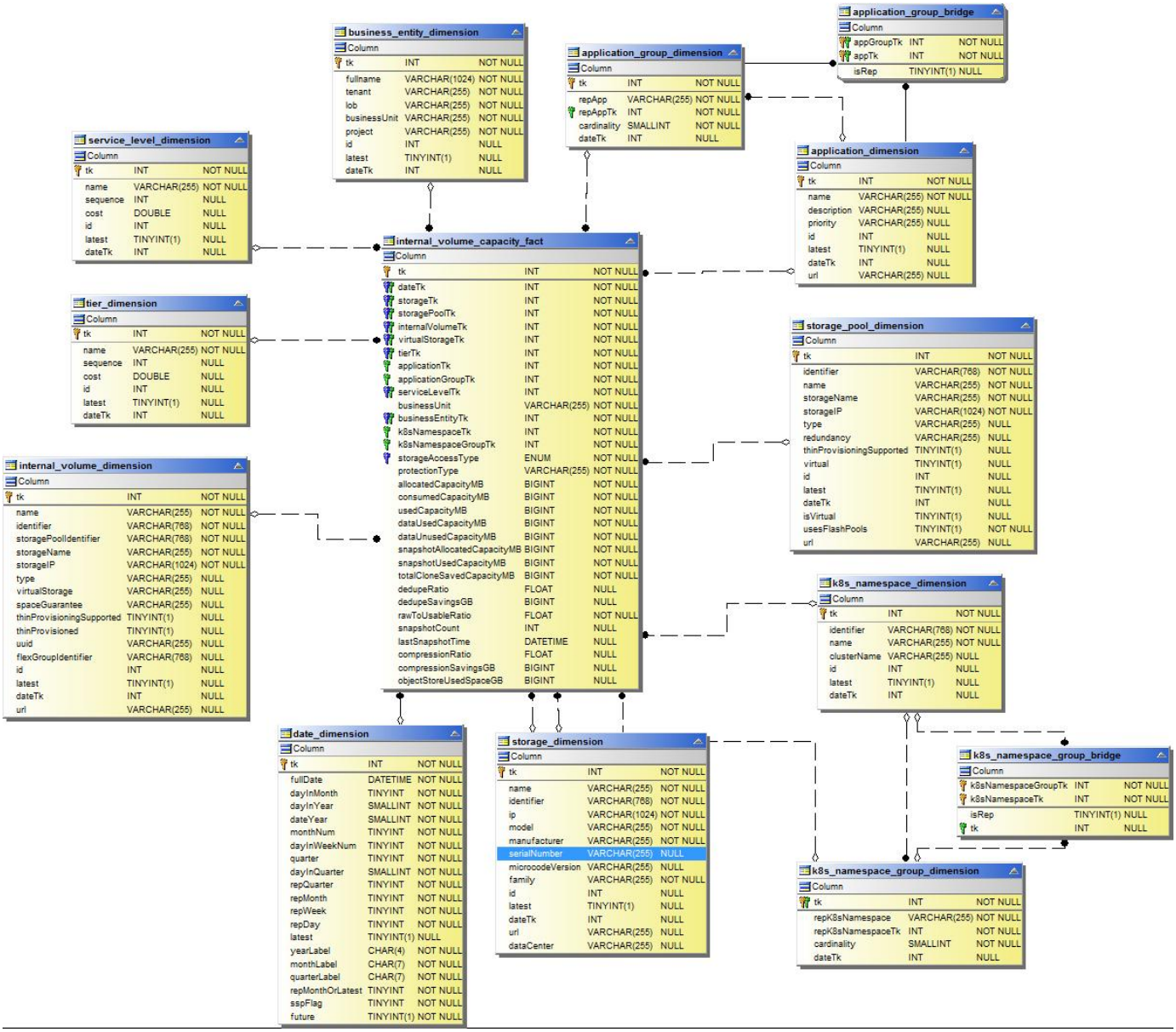
Capacità del gruppo di dischi



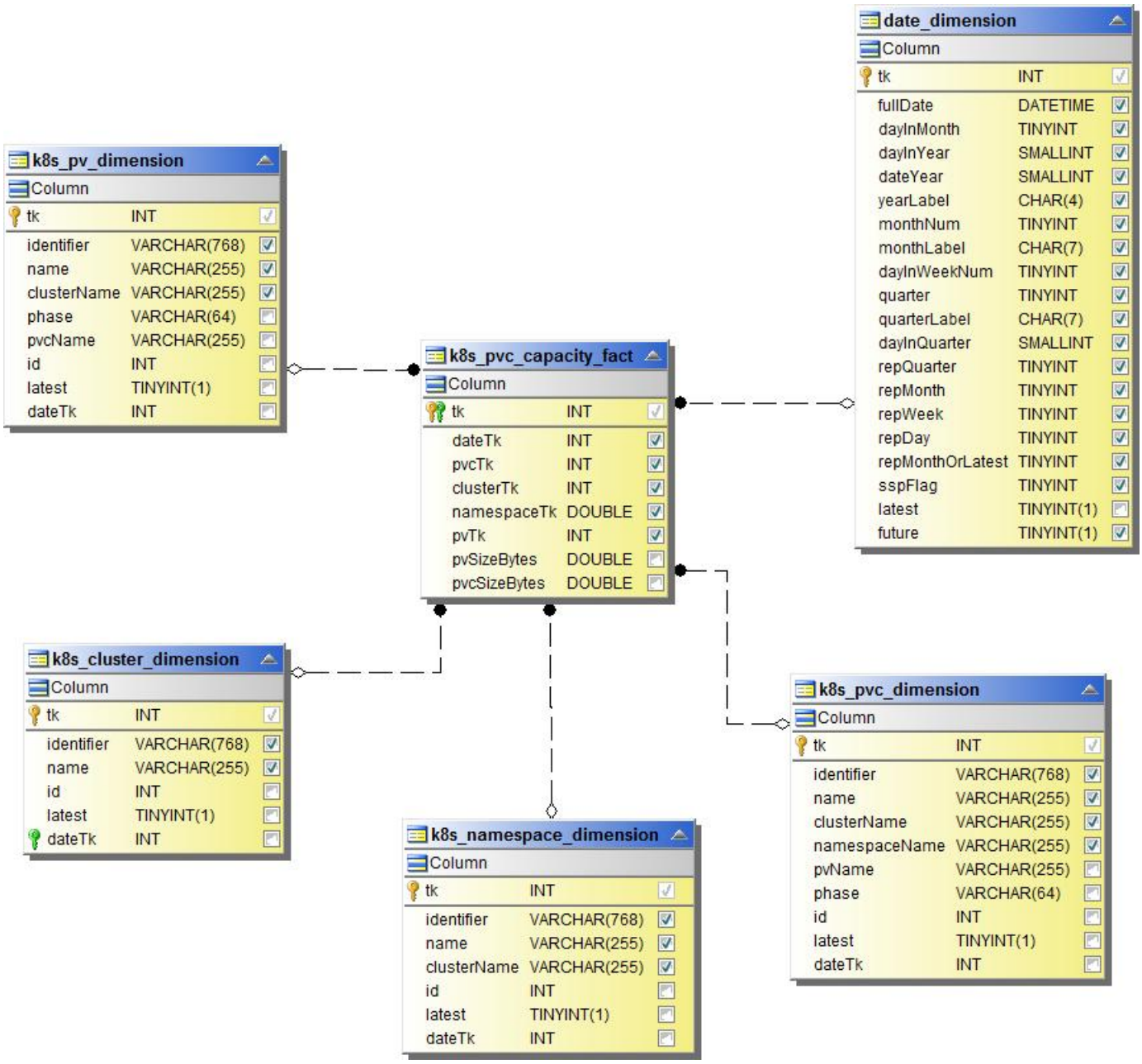
Utilizzo del file system



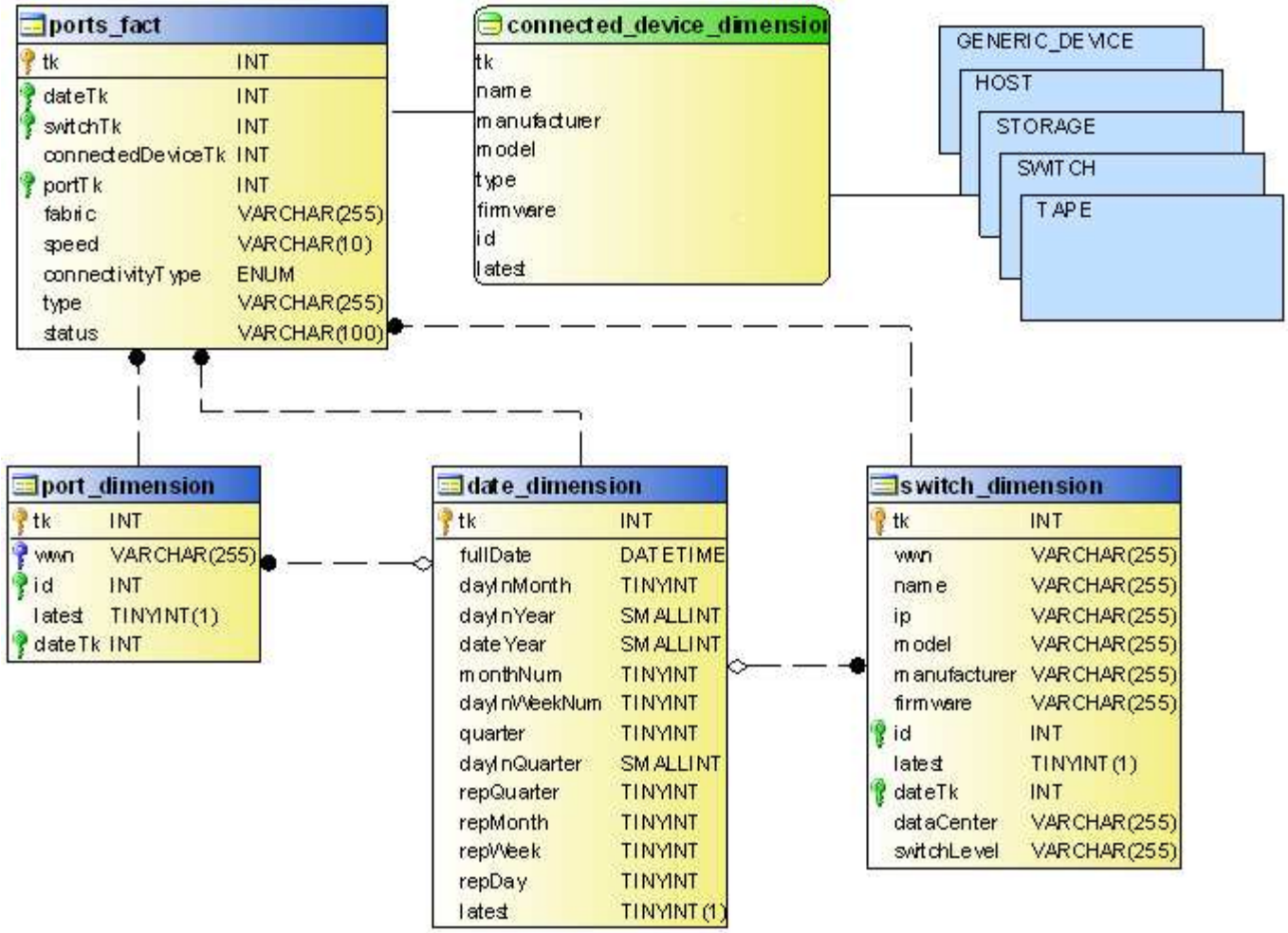
Capacità di volume interno



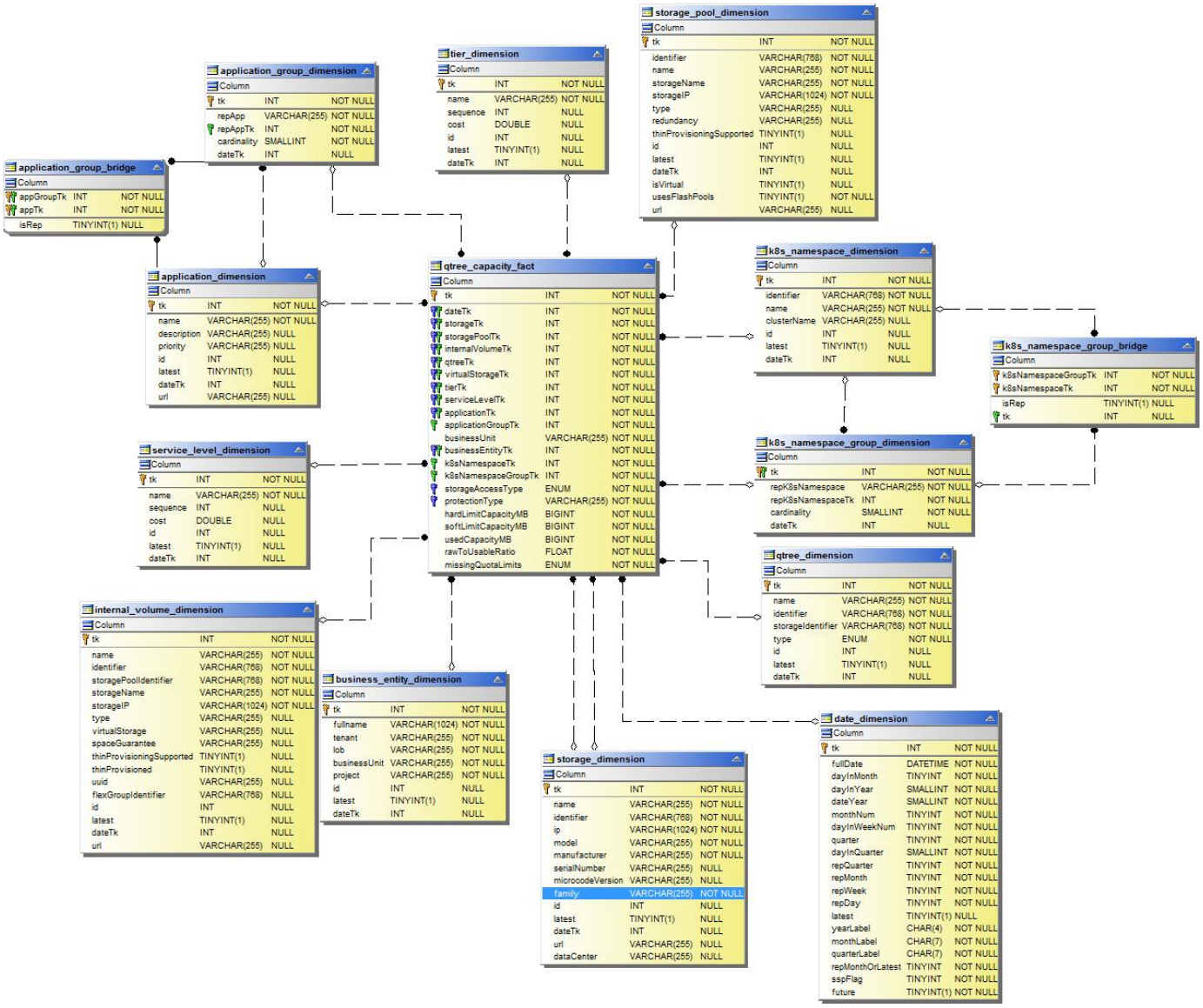
Capacità fotovoltaica di Kubernetes



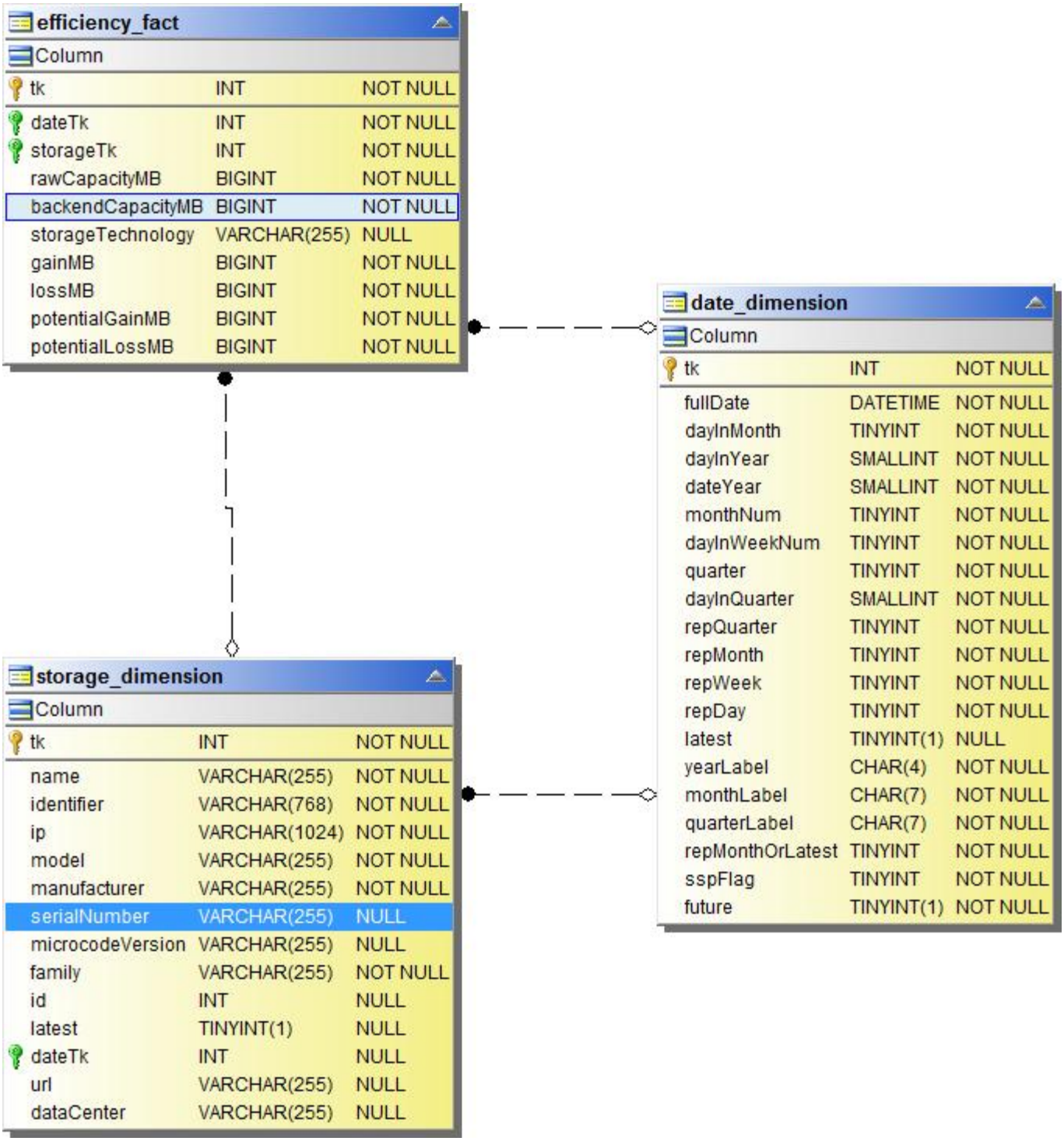
Capacità del porto



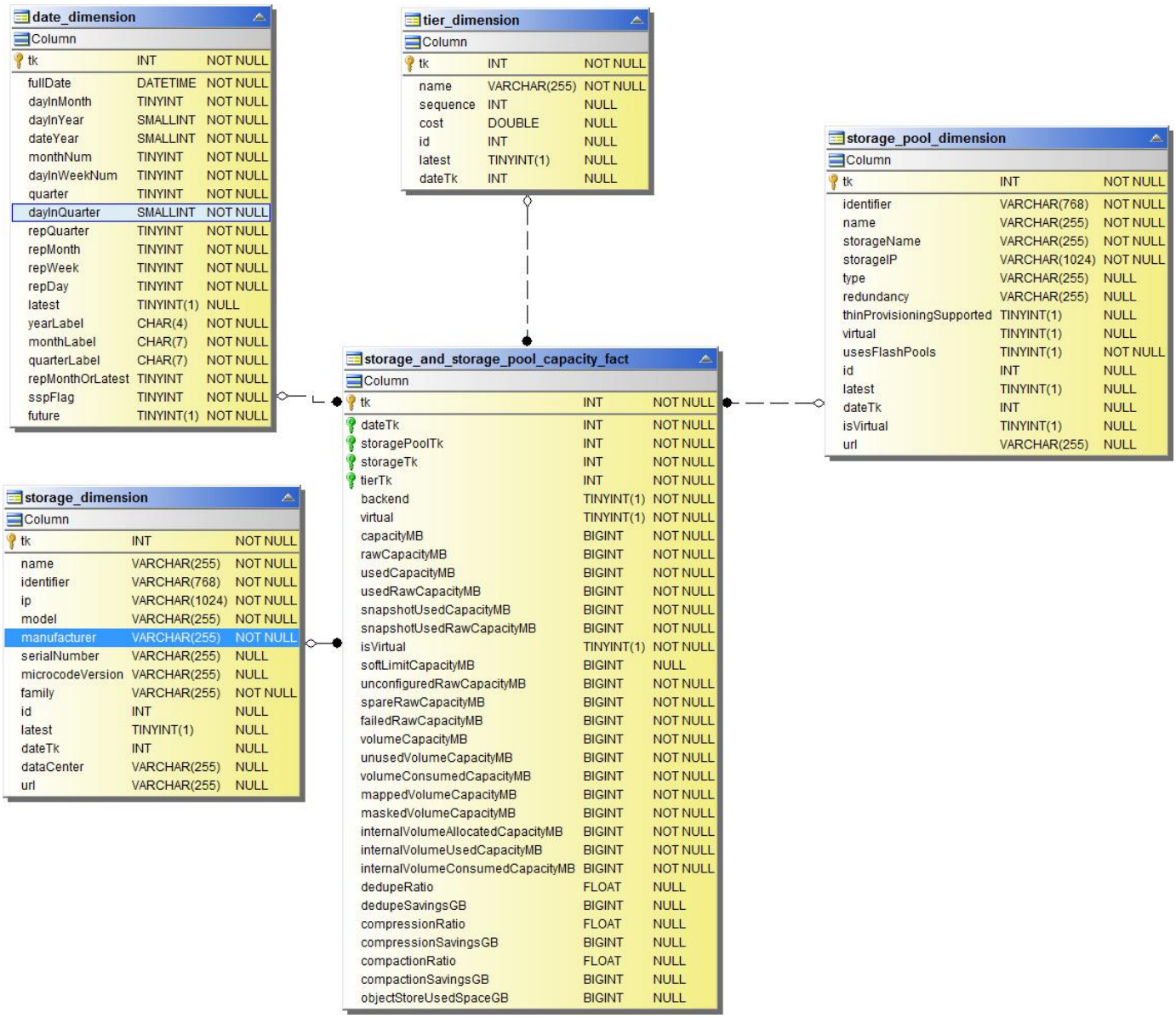
Capacità Qtree



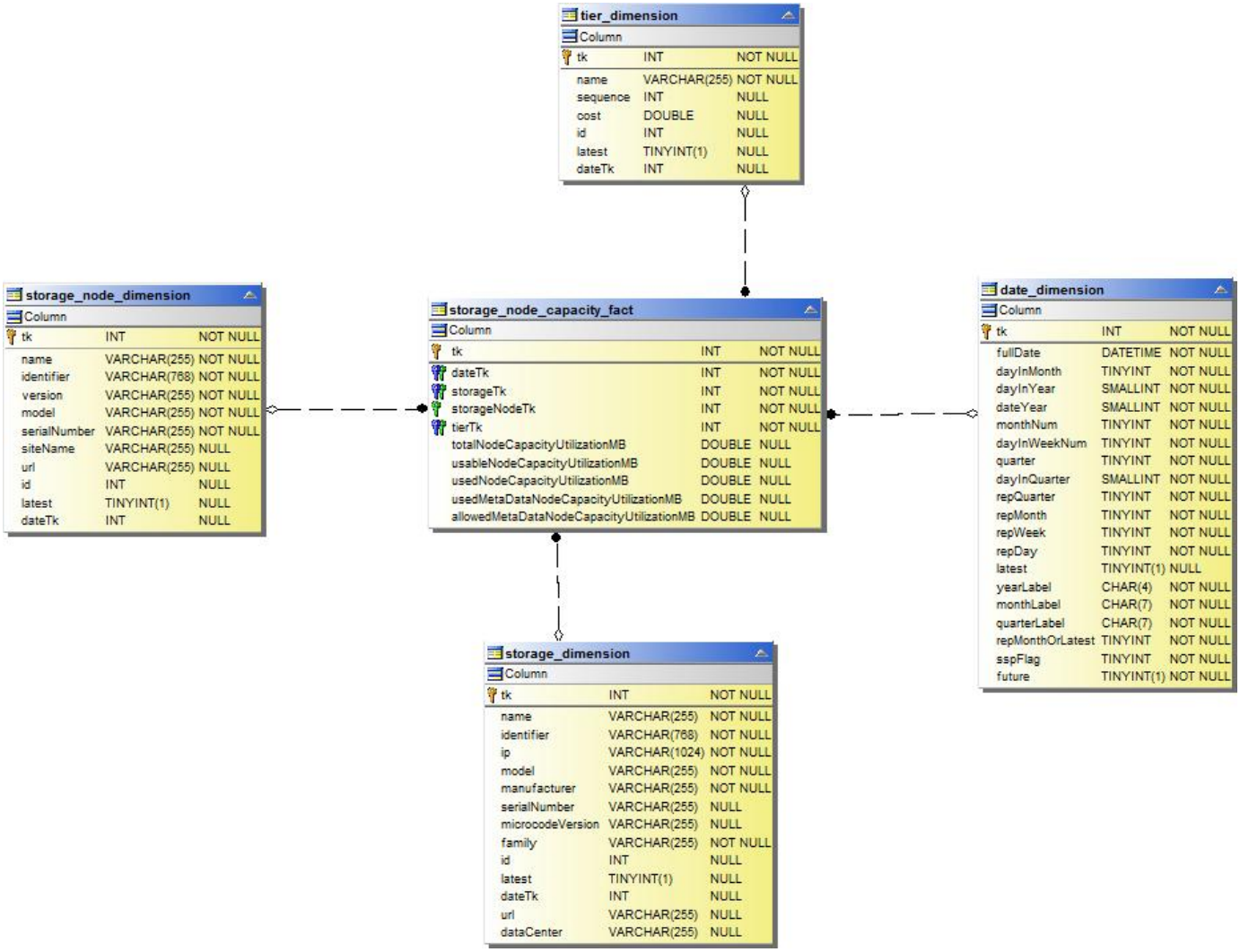
Efficienza della capacità di archiviazione



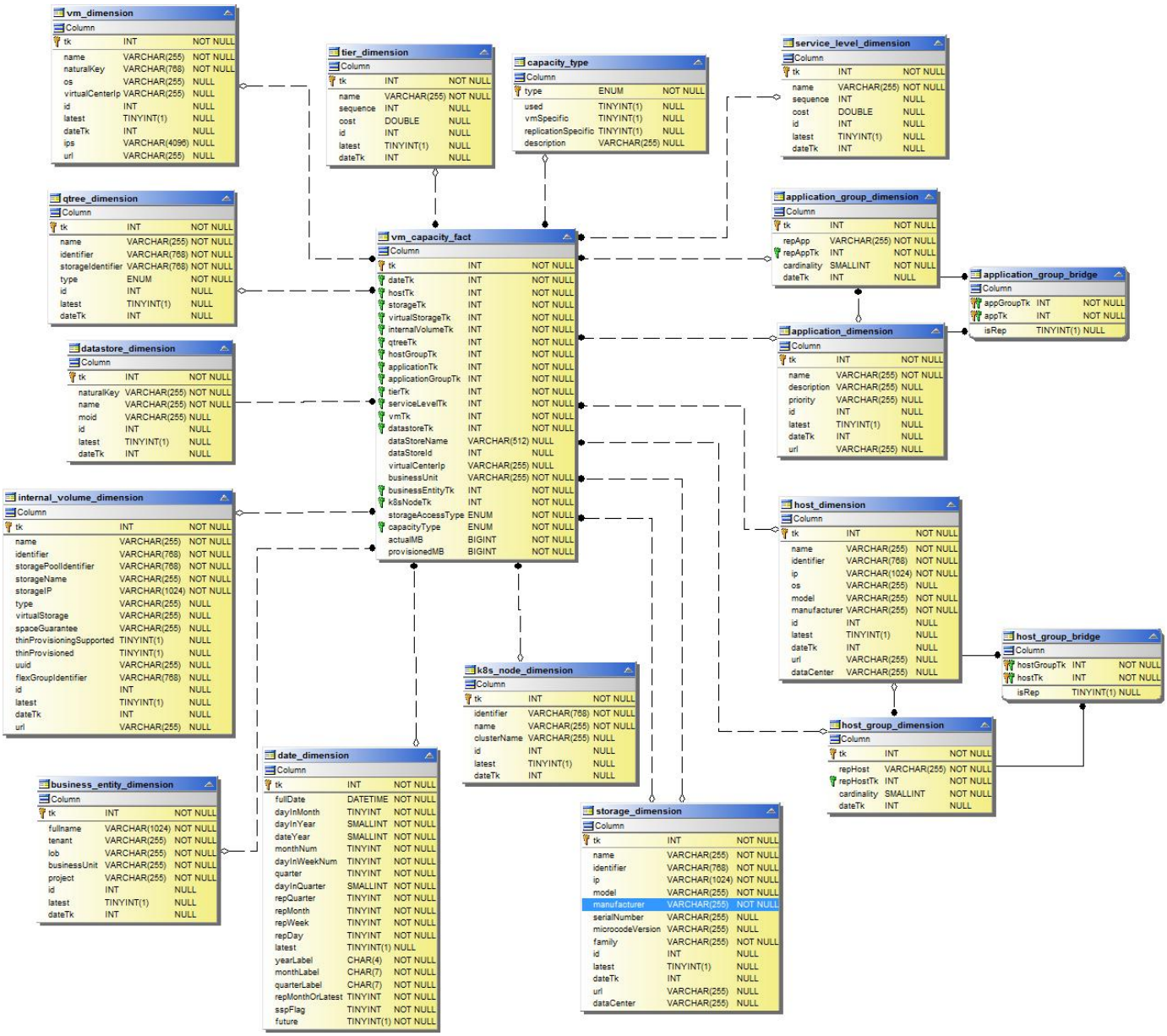
Capacità di stoccaggio e pool di stoccaggio



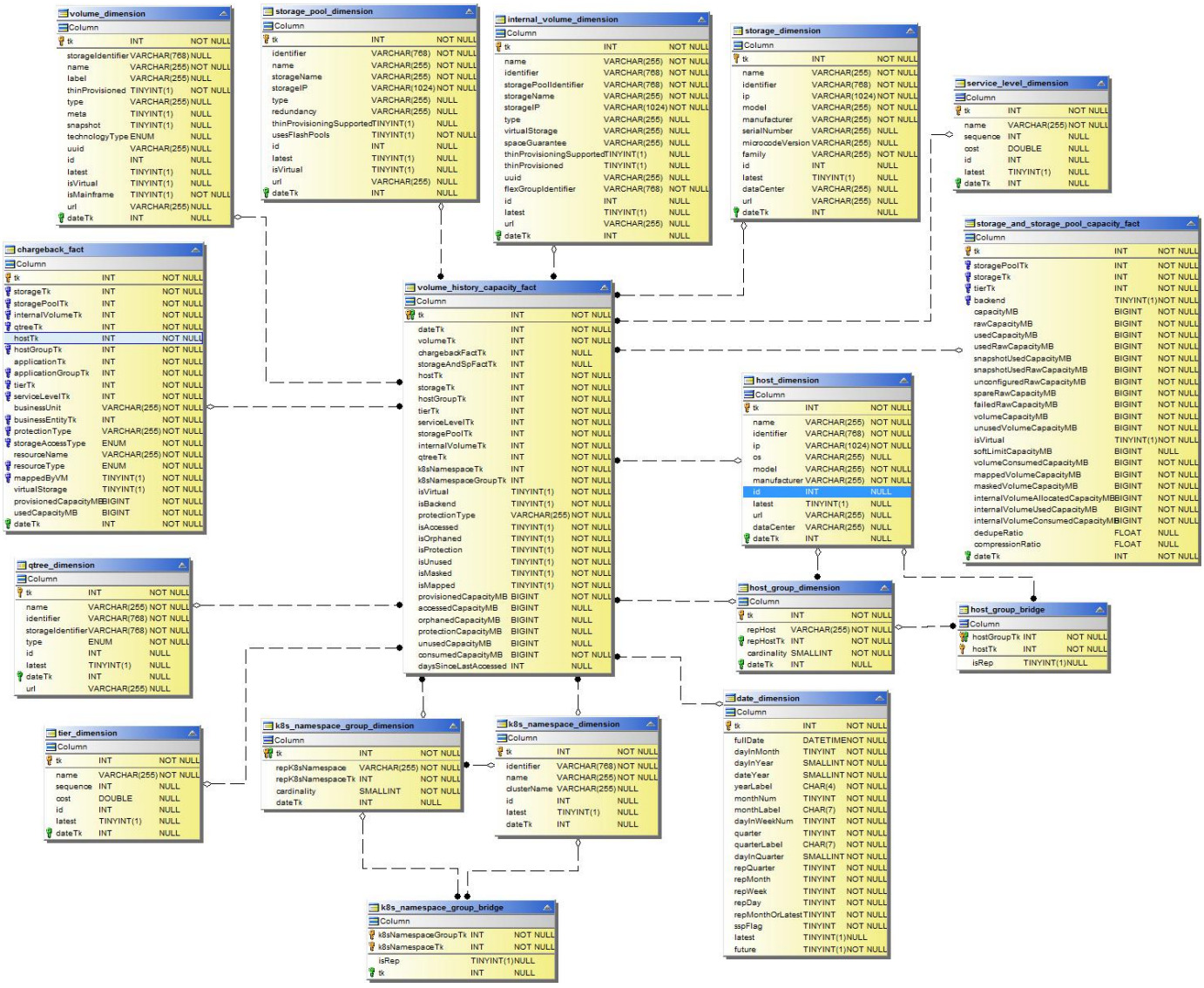
Capacità del nodo di archiviazione



Capacità della VM



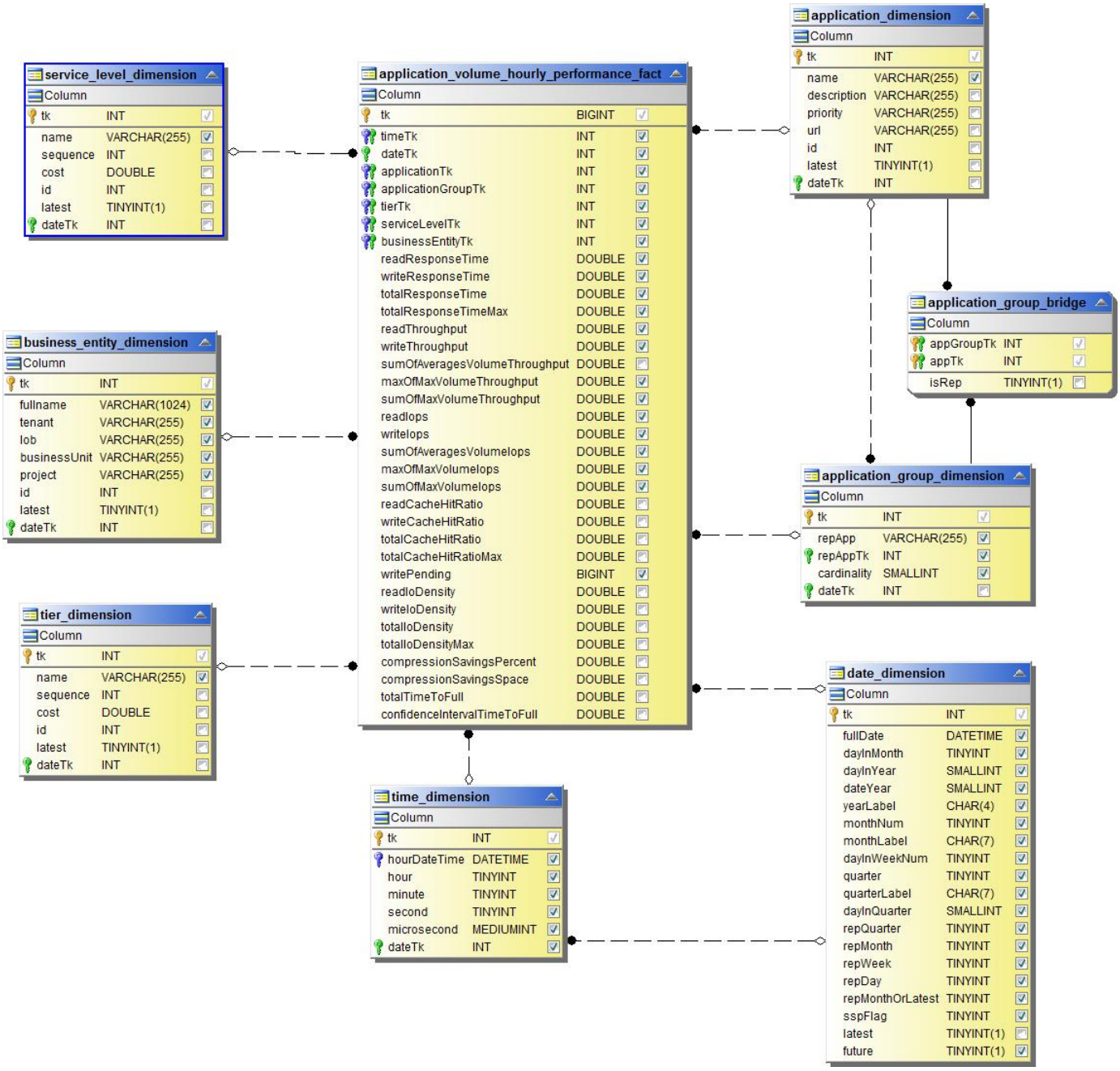
Capacità di volume



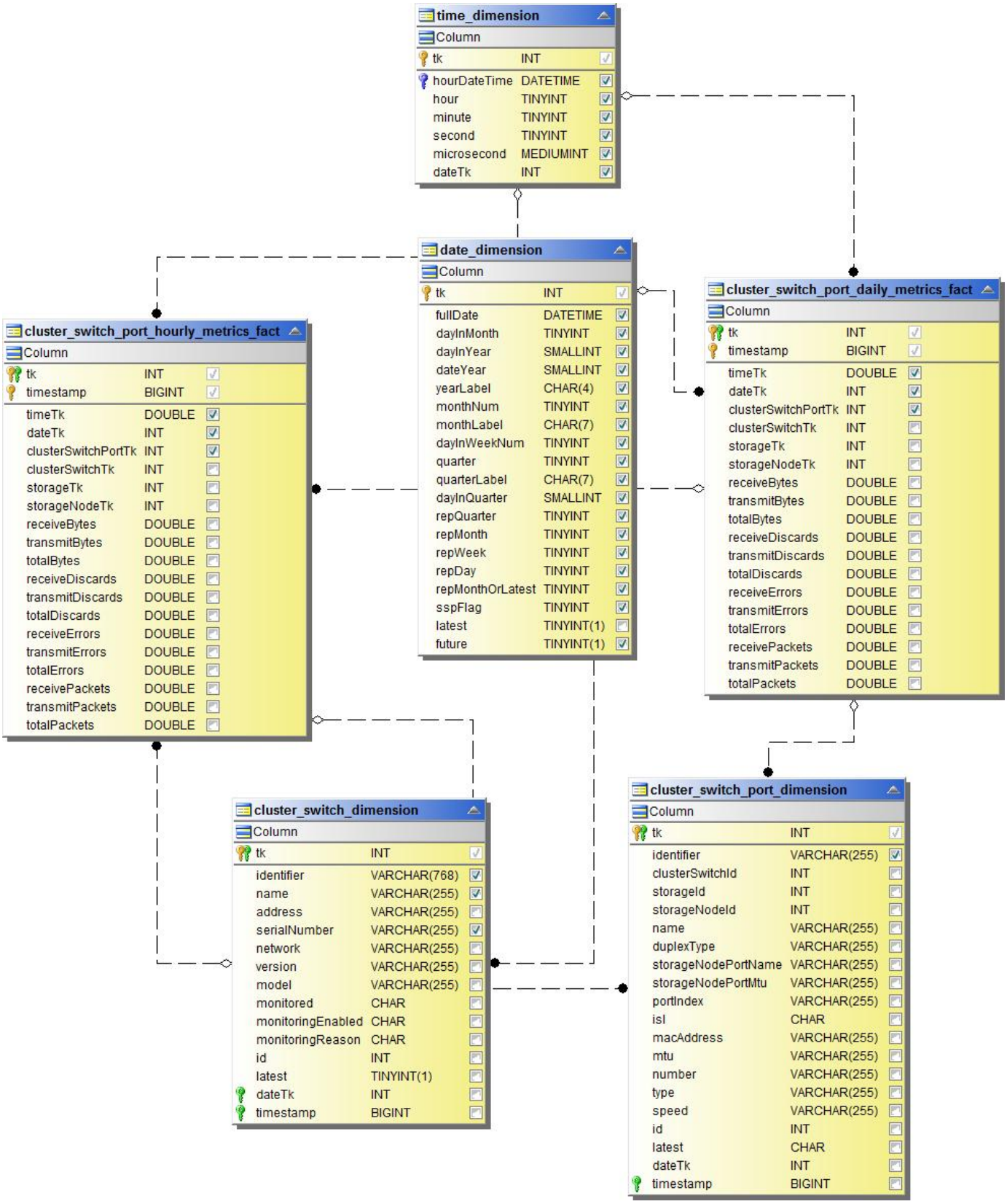
Performance Datamart

Le immagini seguenti descrivono il datamart delle prestazioni.

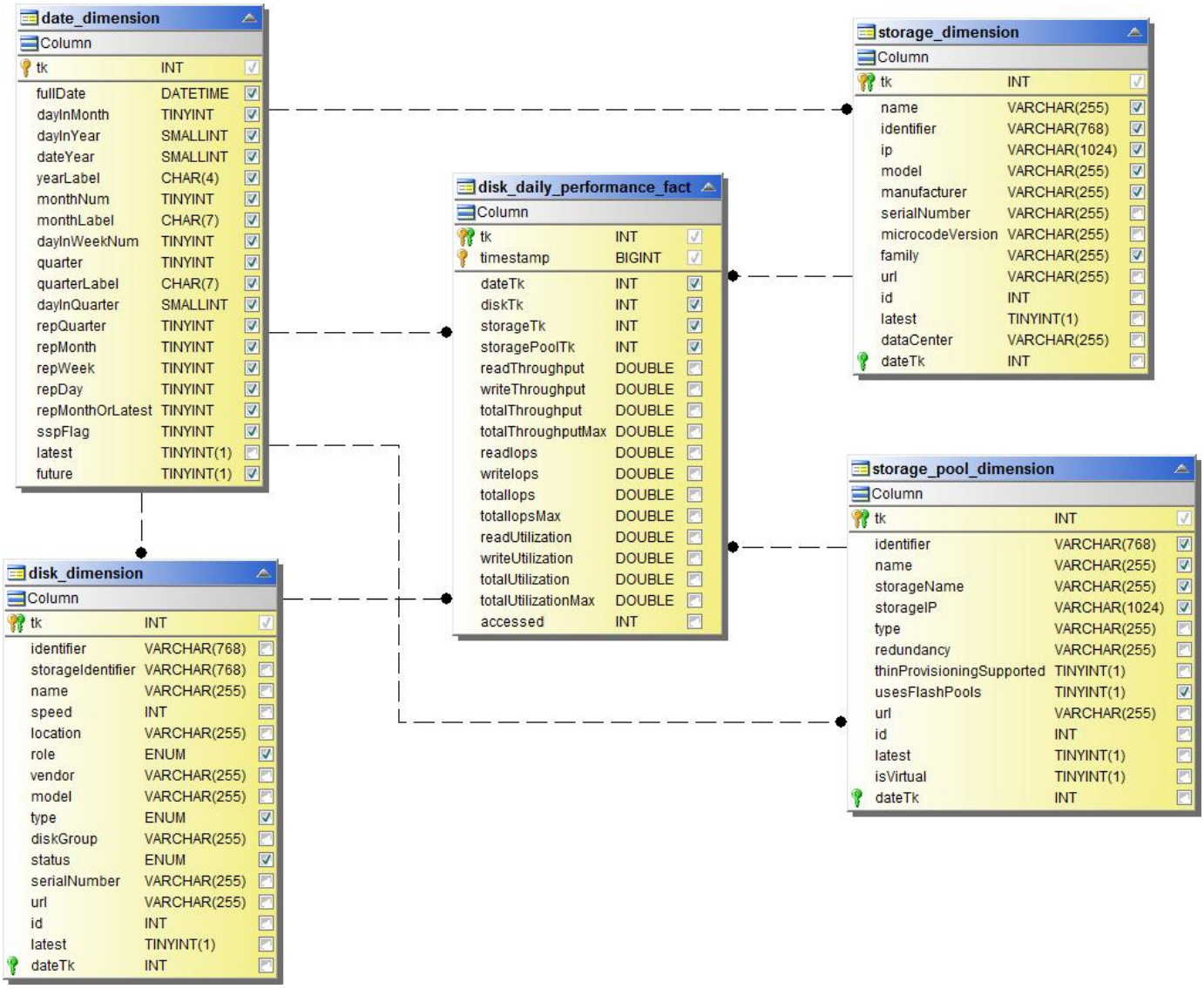
Prestazioni orarie del volume dell'applicazione



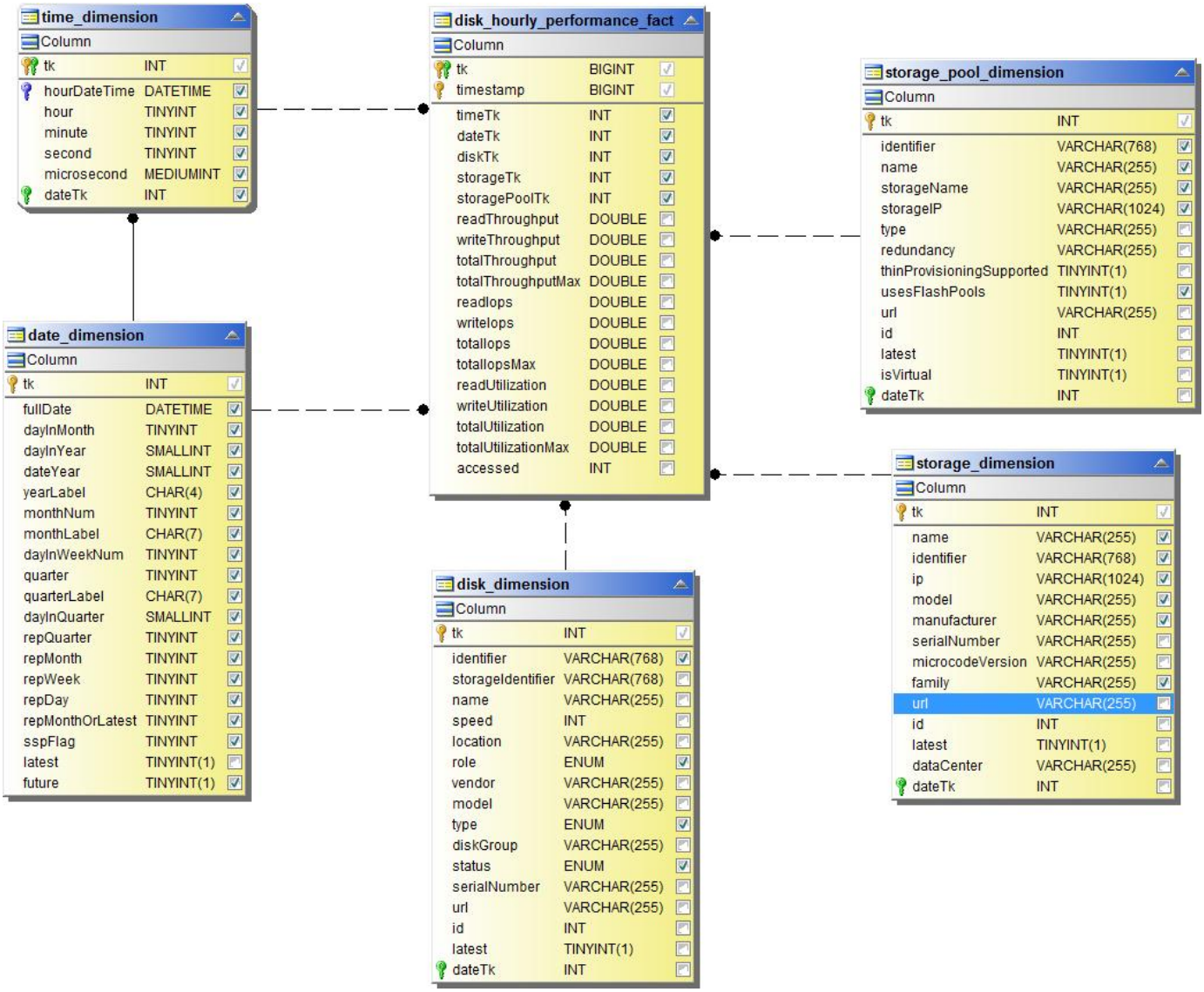
Prestazioni dello switch cluster



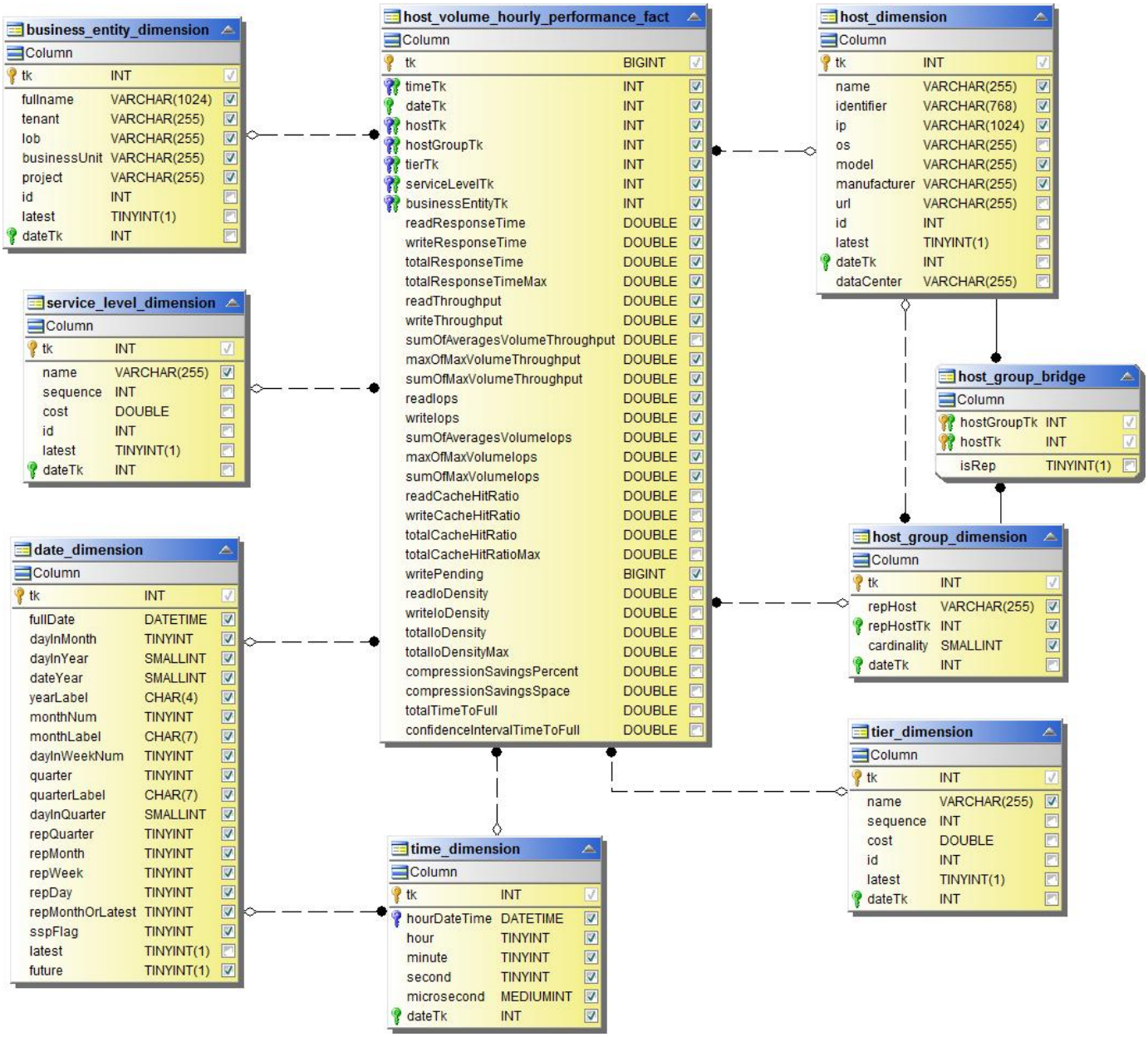
Prestazioni giornaliere del disco



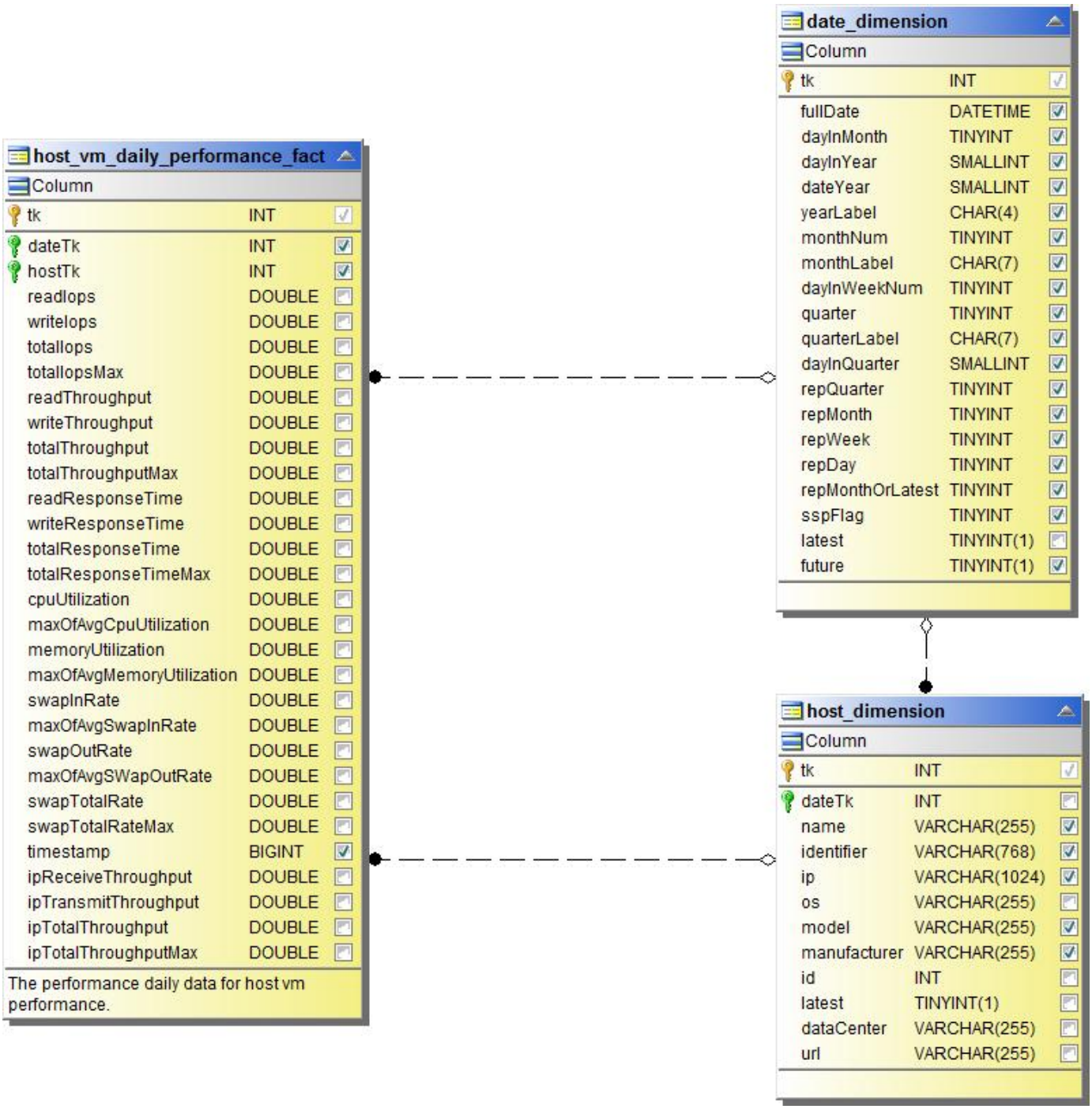
Prestazioni orarie del disco



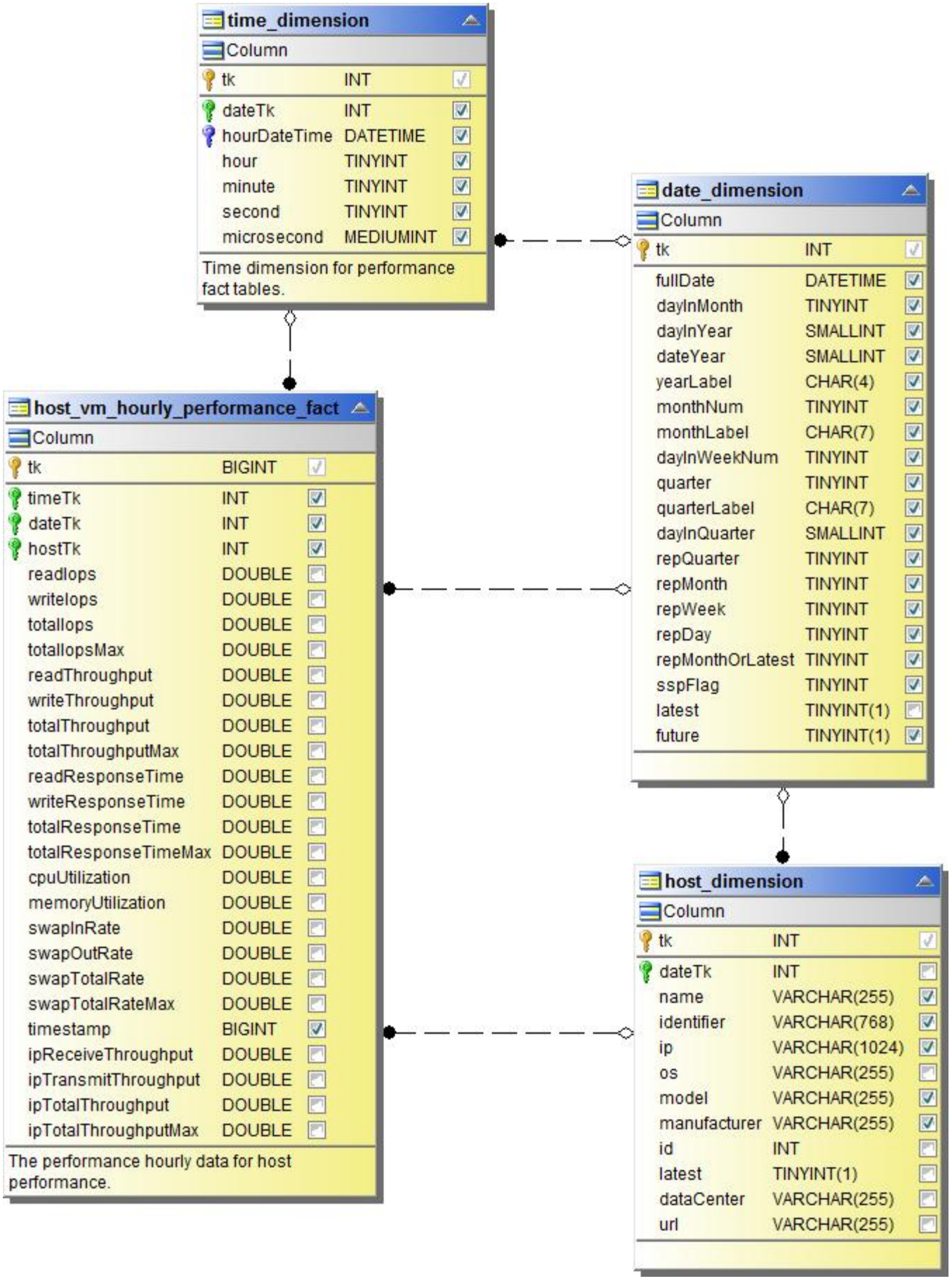
Prestazioni orarie dell'host



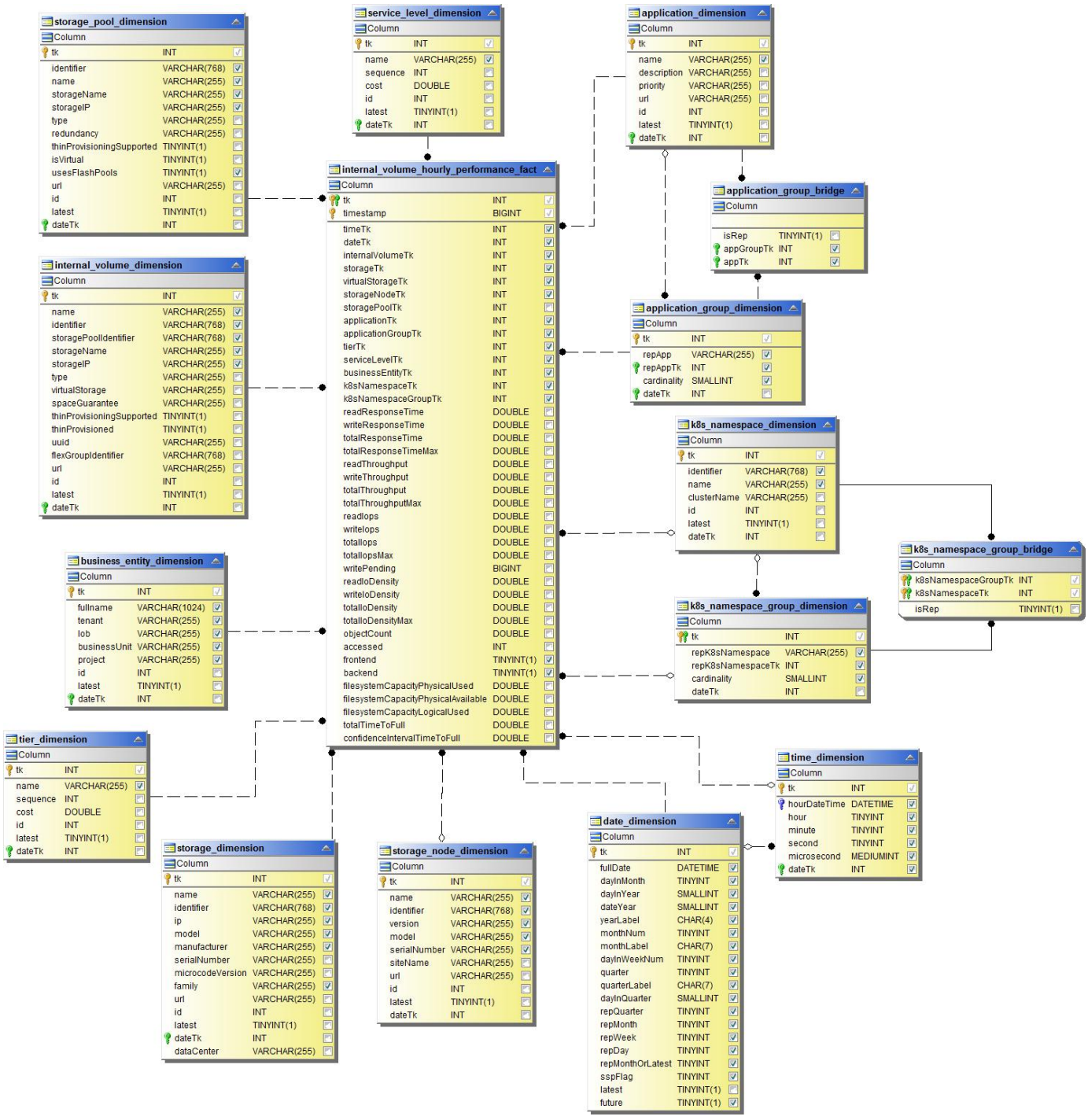
Prestazioni giornaliere della VM host



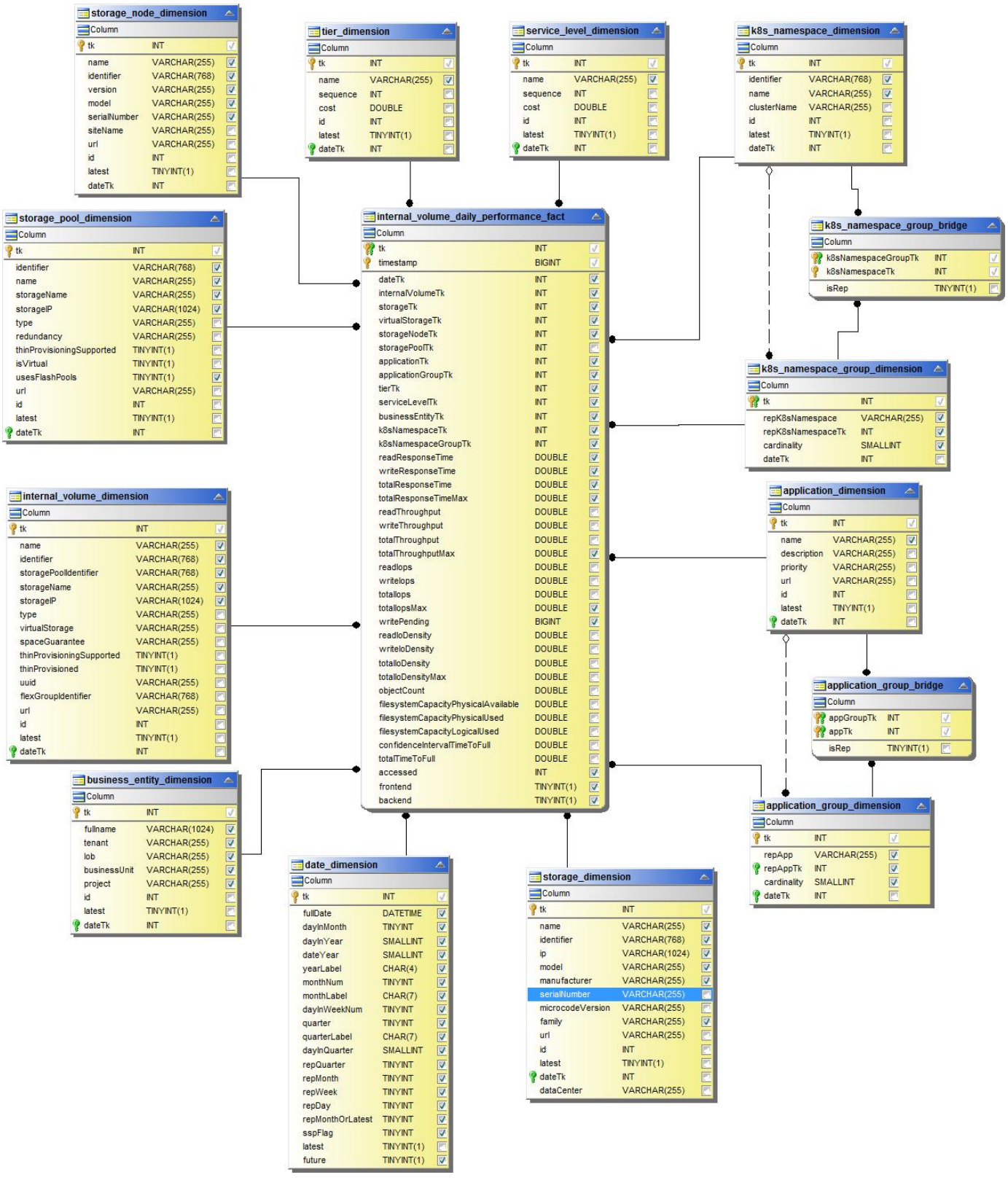
Prestazioni orarie della VM host


time_dimension
Column
tk INT
dateTk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
Time dimension for performance fact tables.
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
host_vm_hourly_performance_fact
Column
tk BIGINT
timeTk INT
dateTk INT
hostTk INT
readIops DOUBLE
writeIops DOUBLE
totalIops DOUBLE
totalIopsMax DOUBLE
readThroughput DOUBLE
writeThroughput DOUBLE
totalThroughput DOUBLE
totalThroughputMax DOUBLE
readResponseTime DOUBLE
writeResponseTime DOUBLE
totalResponseTime DOUBLE
totalResponseTimeMax DOUBLE
cpuUtilization DOUBLE
memoryUtilization DOUBLE
swapInRate DOUBLE
swapOutRate DOUBLE
swapTotalRate DOUBLE
swapTotalRateMax DOUBLE
timestamp BIGINT
ipReceiveThroughput DOUBLE
ipTransmitThroughput DOUBLE
ipTotalThroughput DOUBLE
ipTotalThroughputMax DOUBLE
The performance hourly data for host performance.
host_dimension
Column
tk INT
dateTk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
id INT
latest TINYINT(1)
dataCenter VARCHAR(255)
url VARCHAR(255)

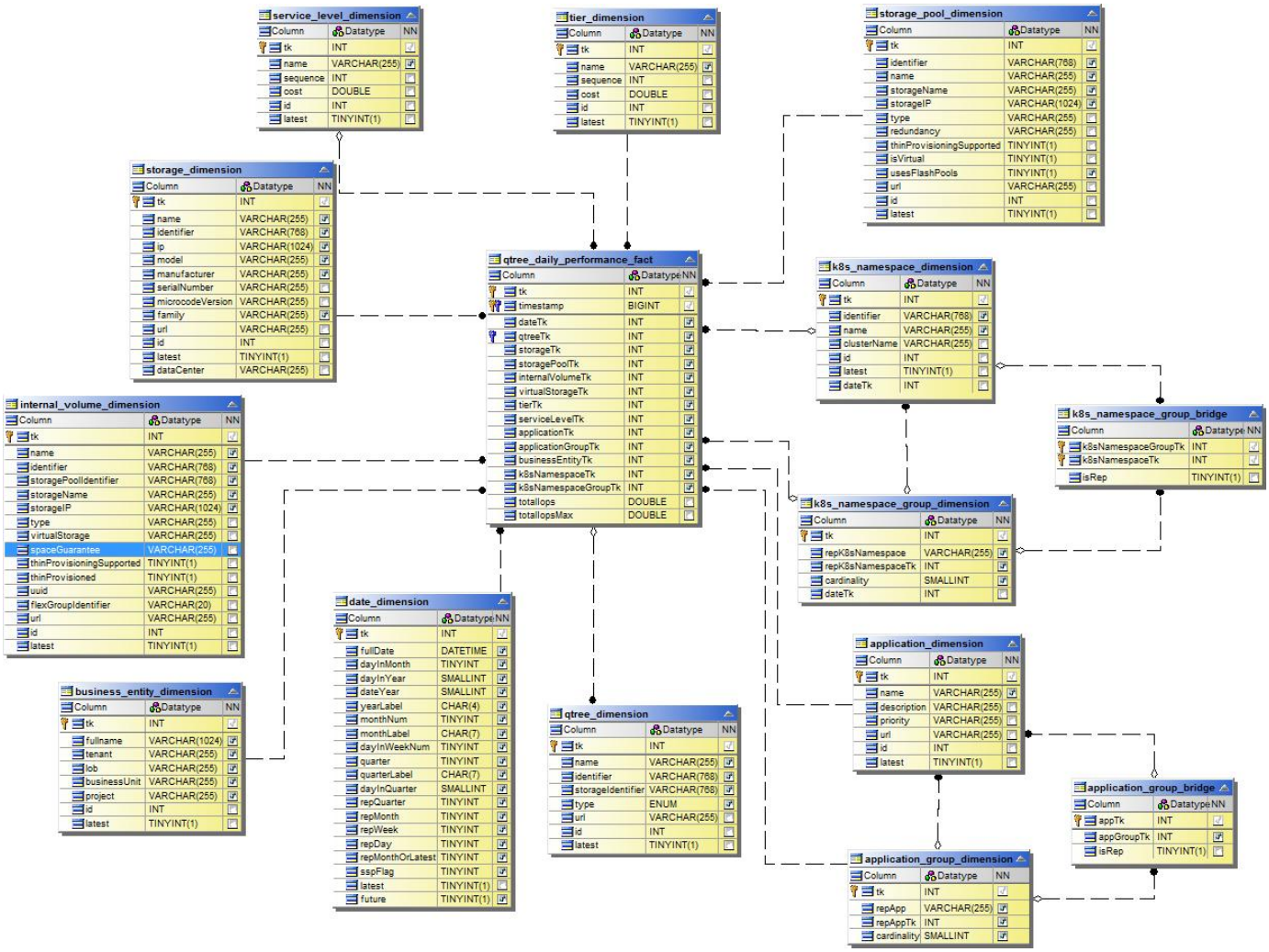
Prestazioni orarie del volume interno



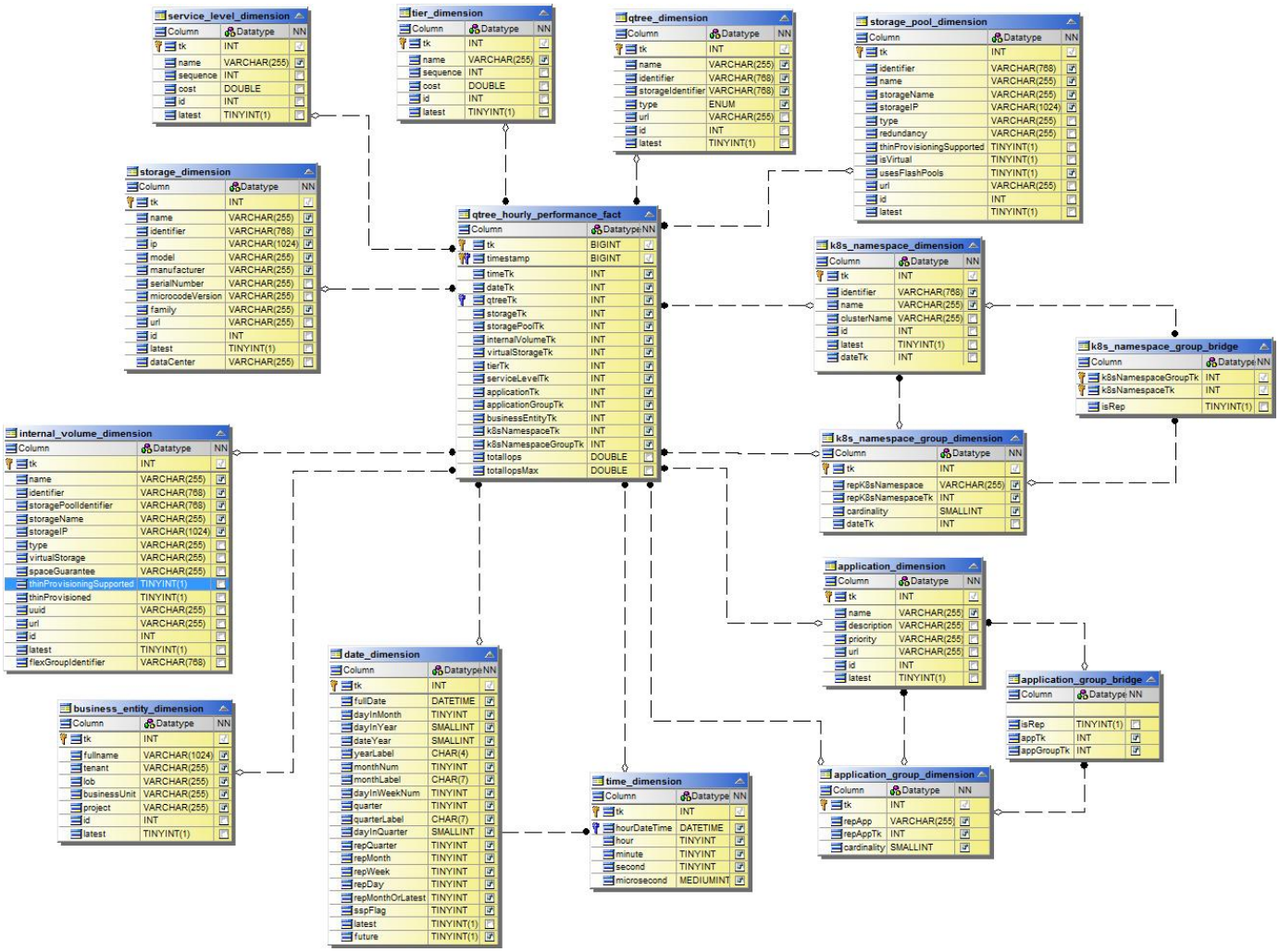
Performance giornaliera del volume interno



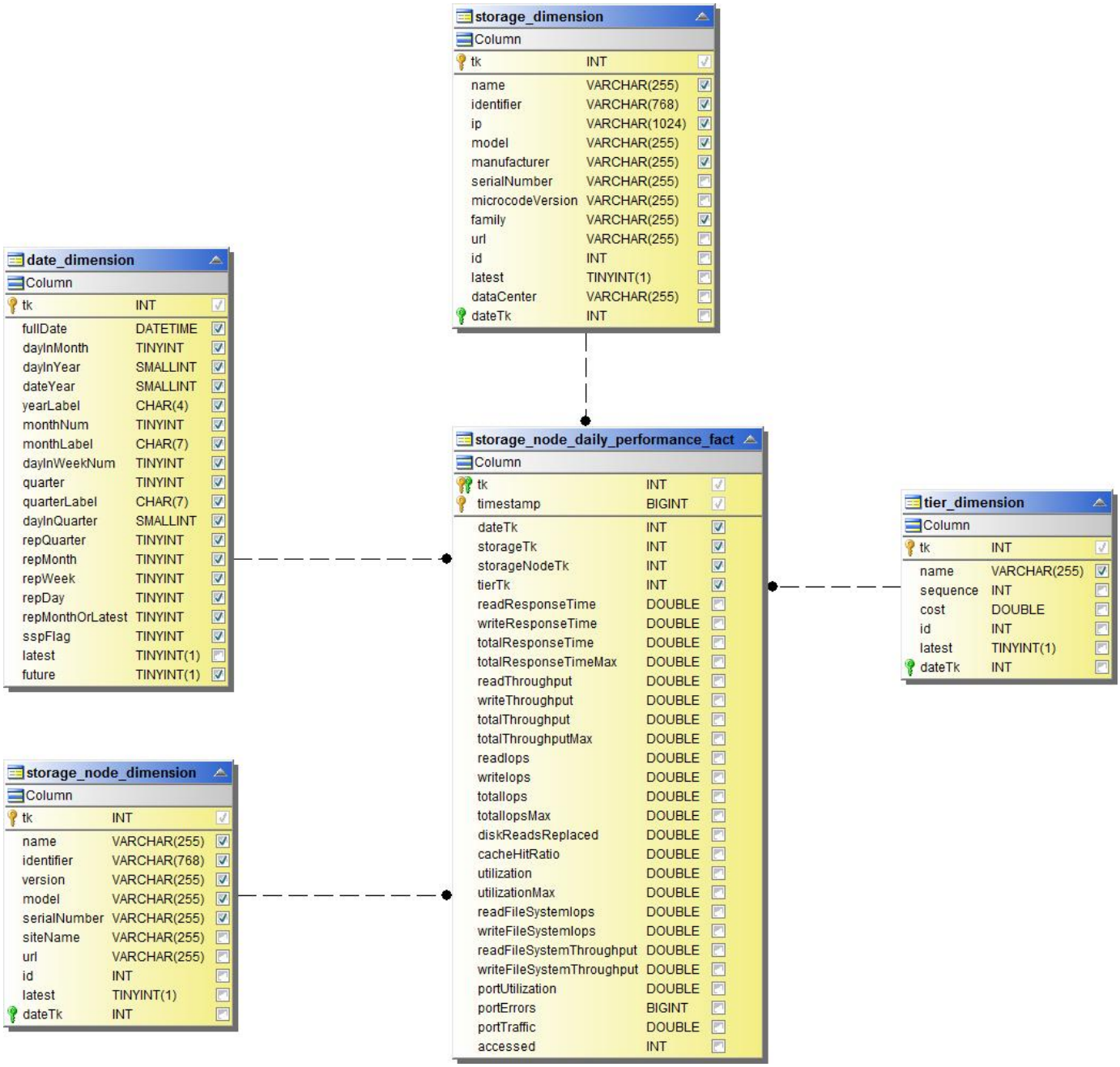
Prestazioni giornaliere di Qtree



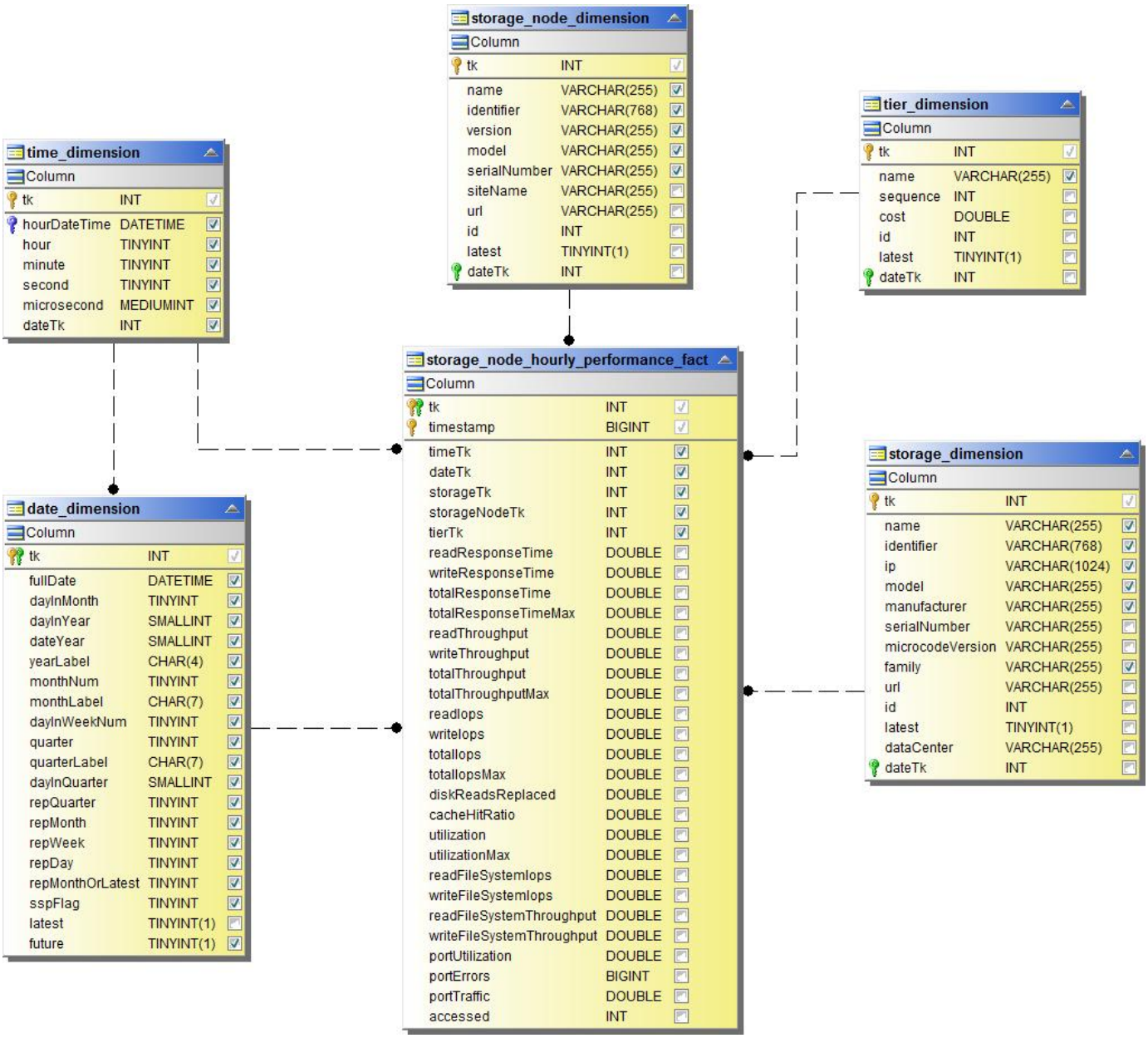
Prestazioni orarie di Qtree



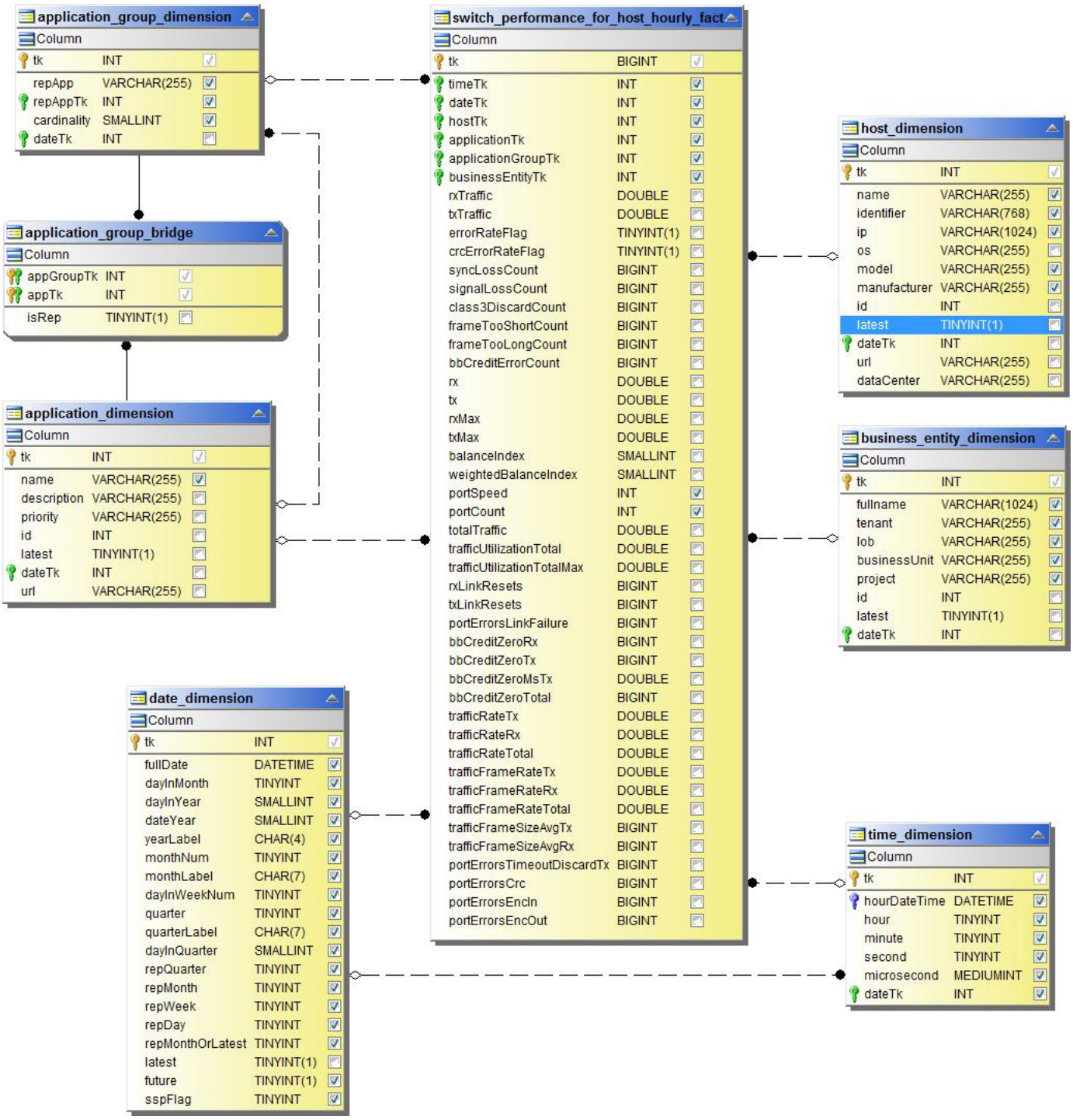
Prestazioni giornaliere del nodo di archiviazione



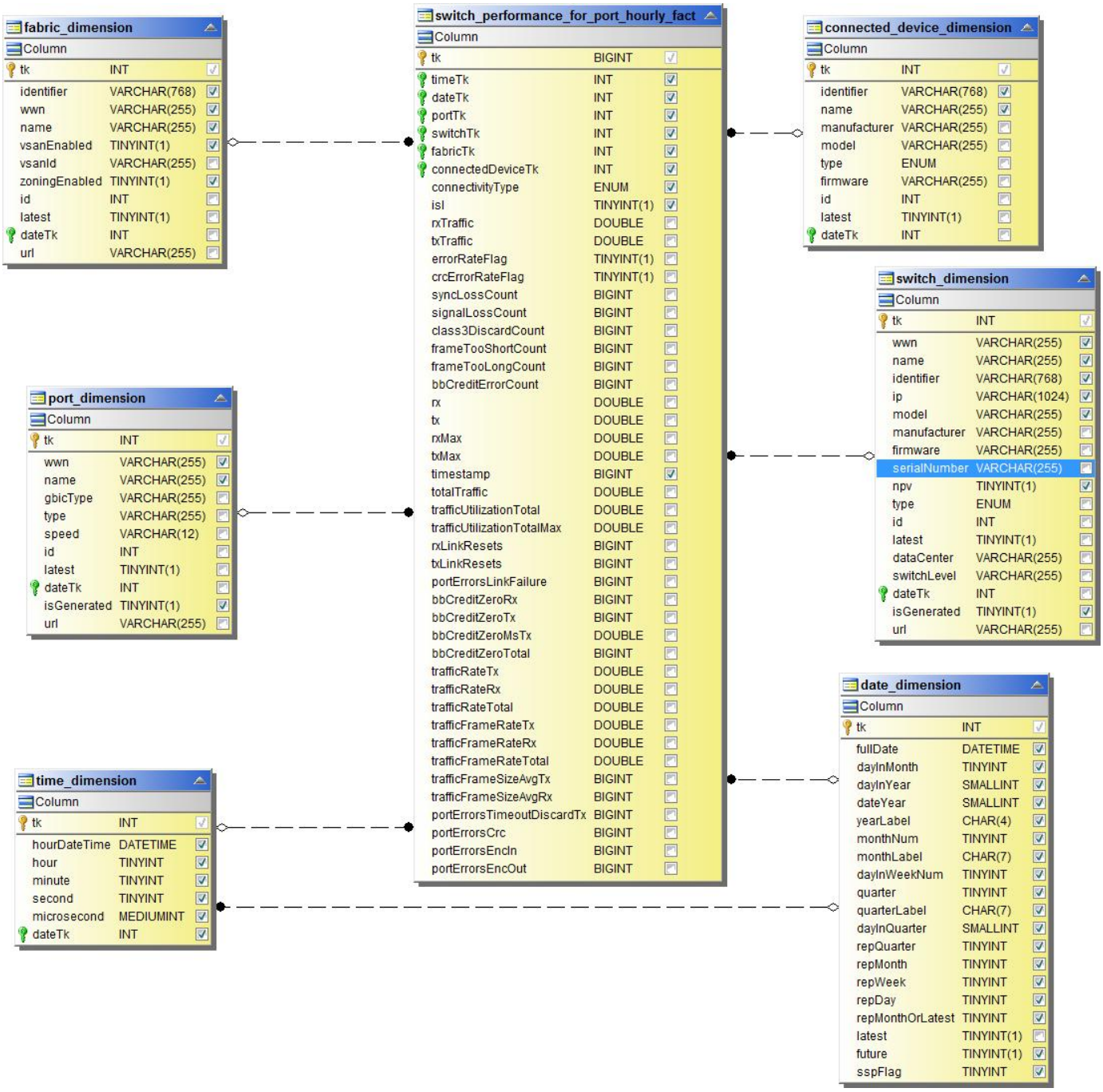
Prestazioni orarie del nodo di archiviazione



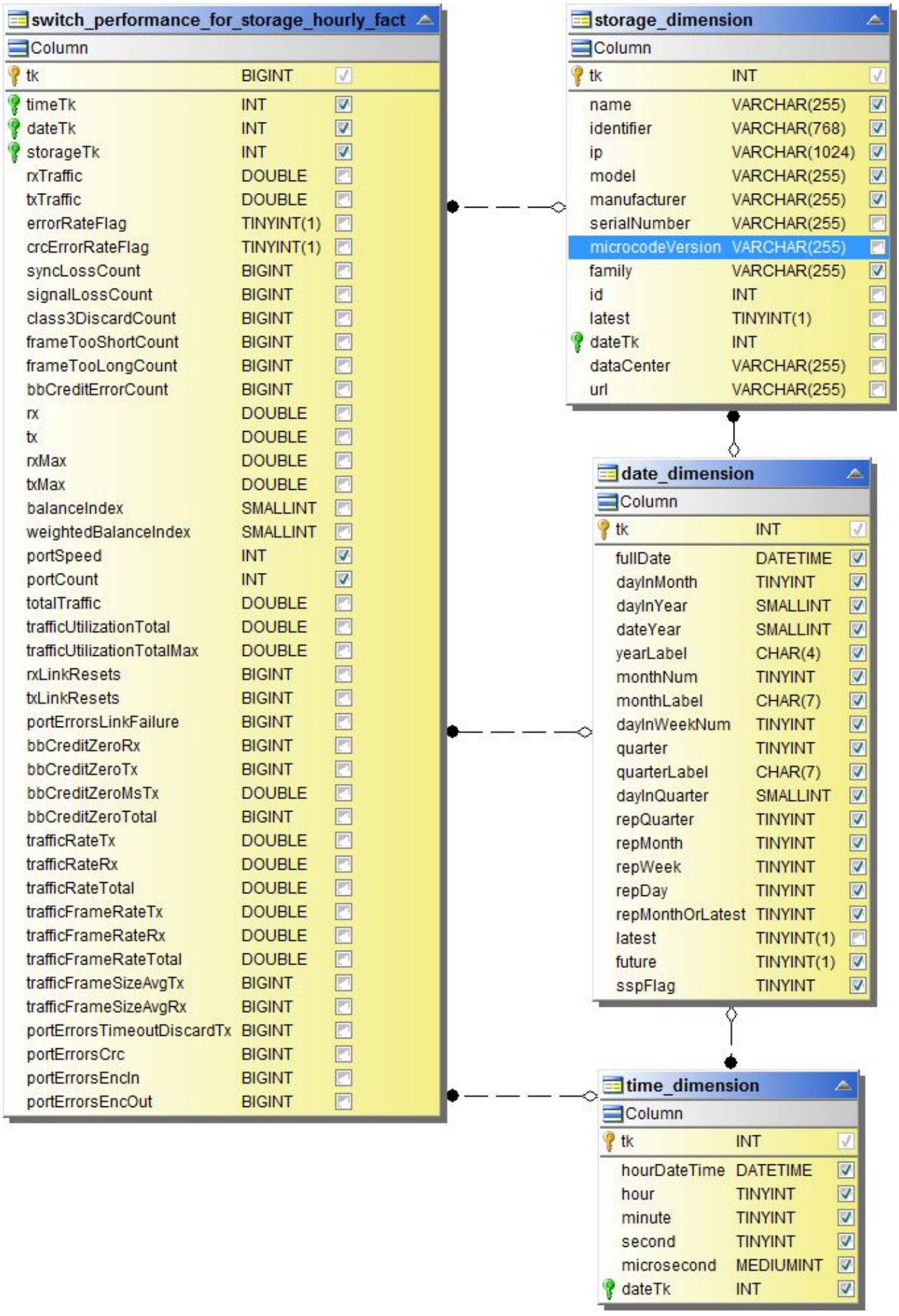
Cambia le prestazioni orarie per l'host



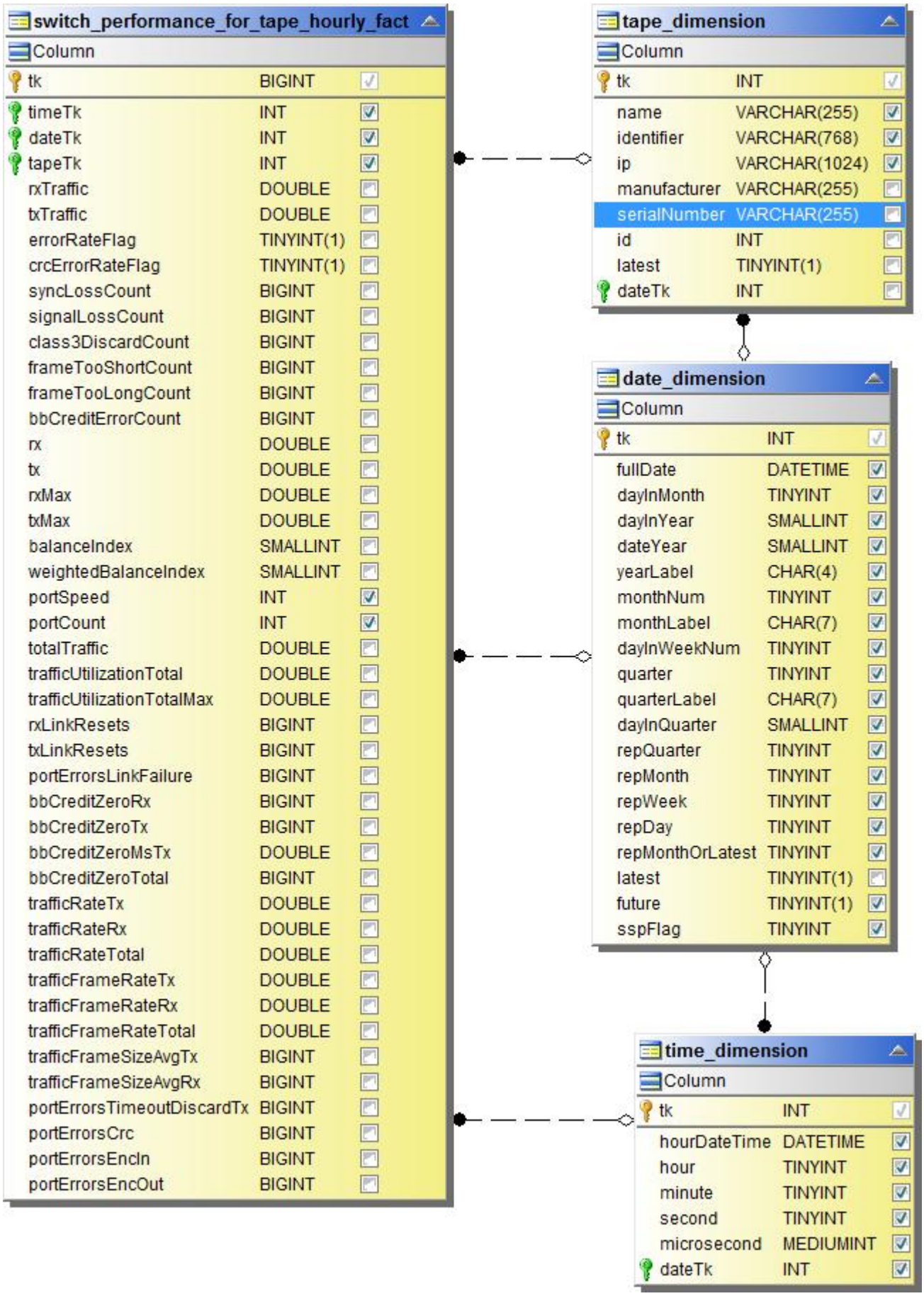
Cambia le prestazioni orarie per porta



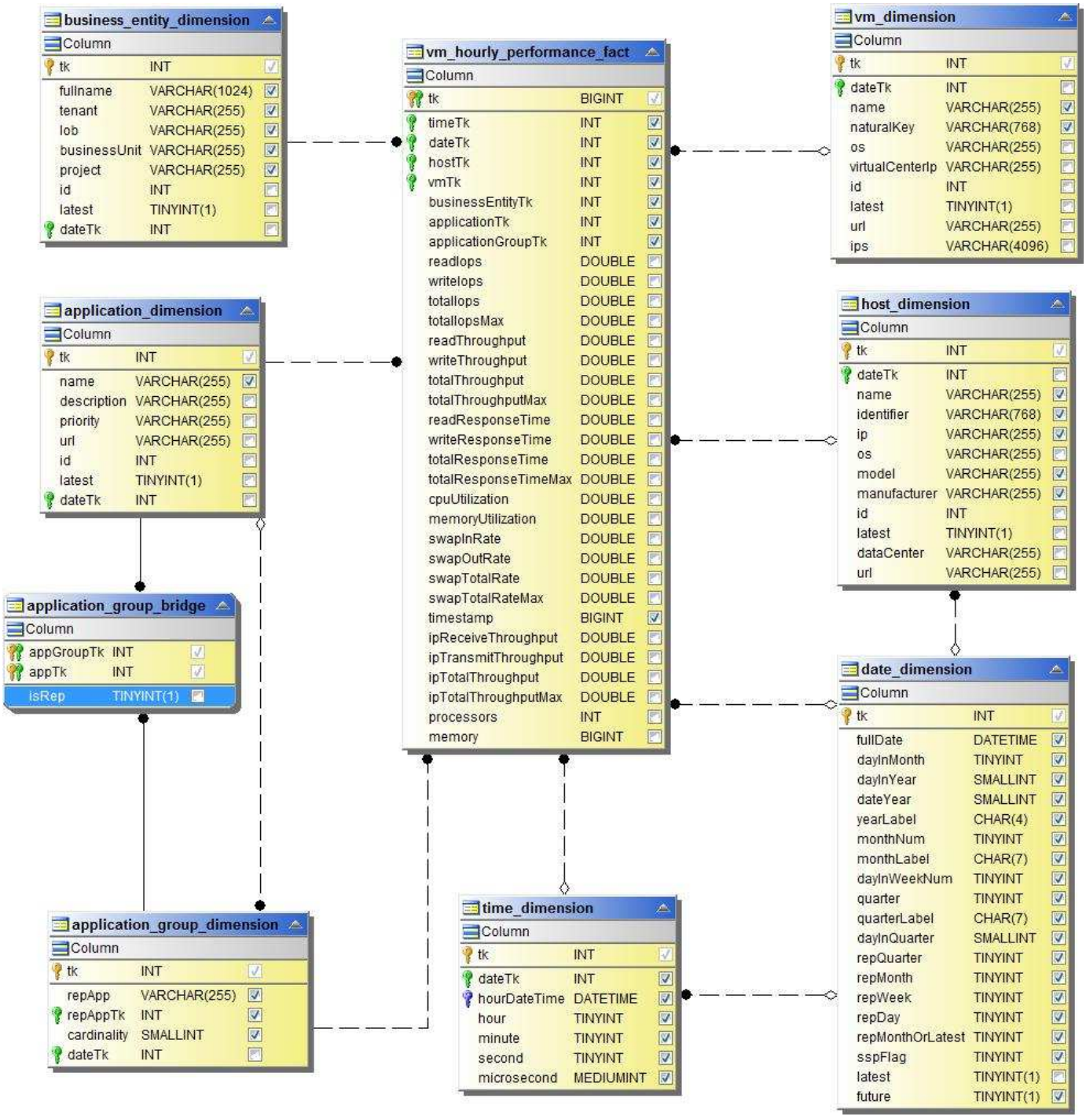
Cambia le prestazioni orarie per l'archiviazione


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

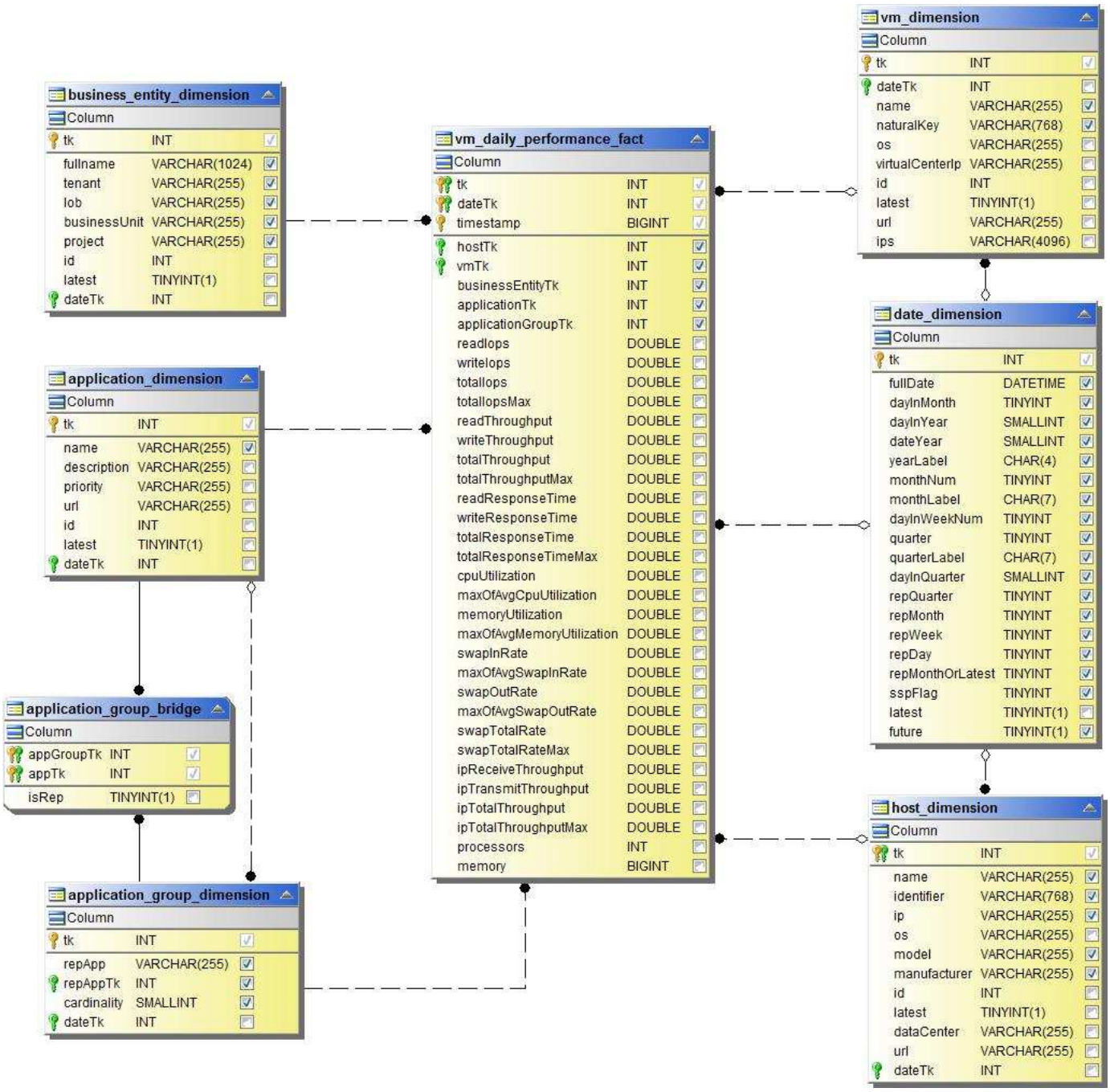
Cambia le prestazioni orarie per il nastro



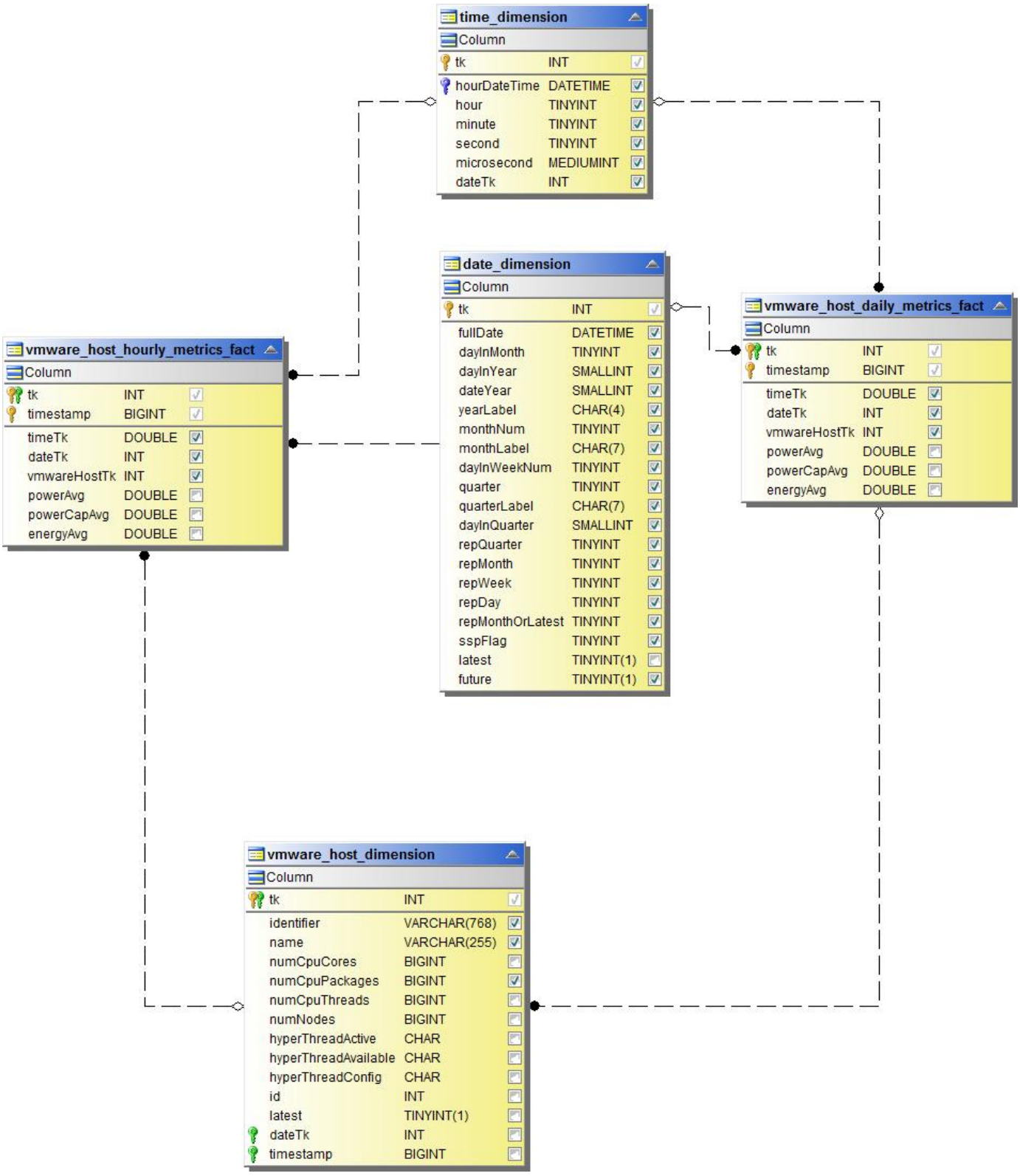
Prestazioni della VM



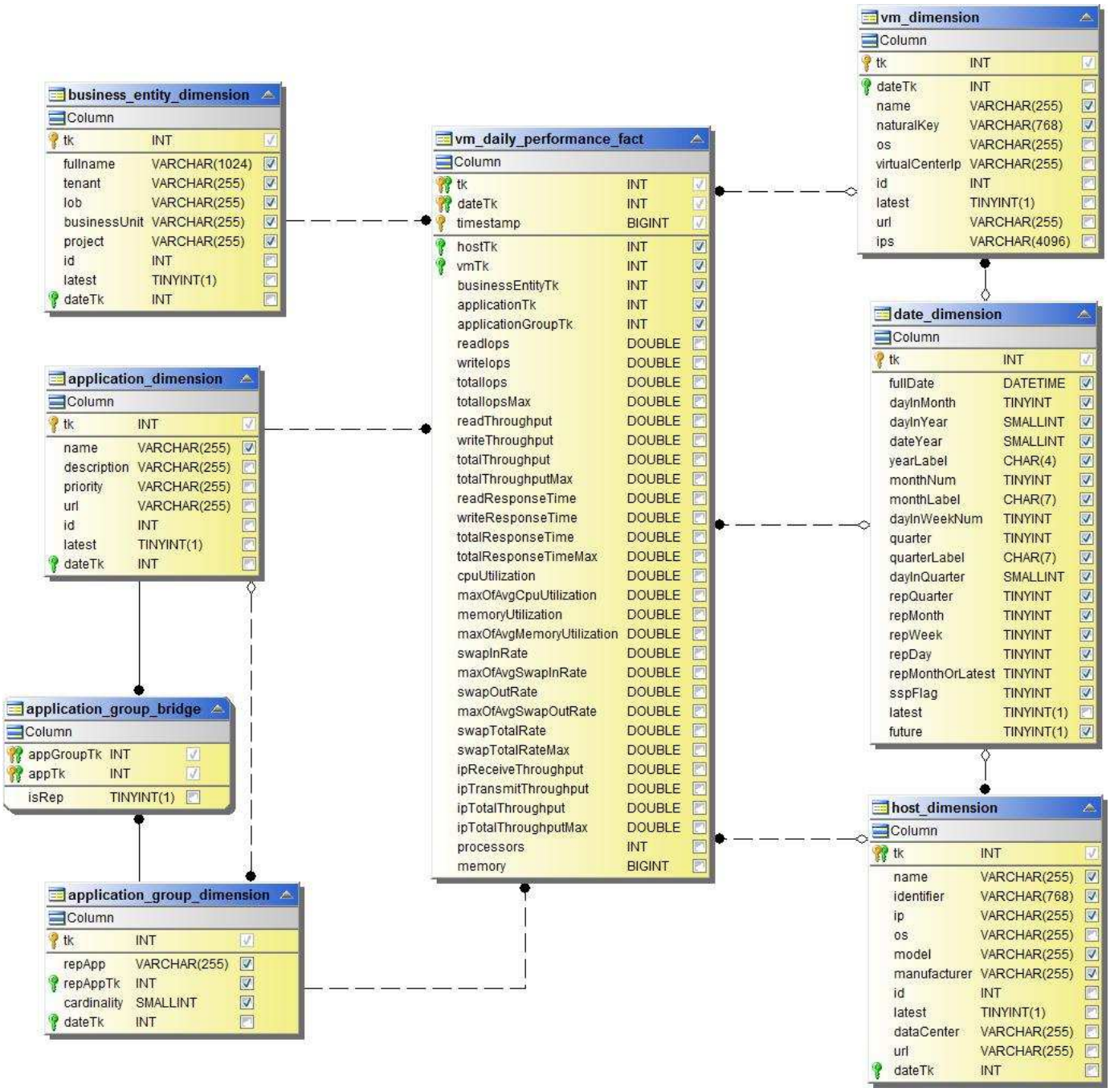
Prestazioni giornaliere della VM per l'host



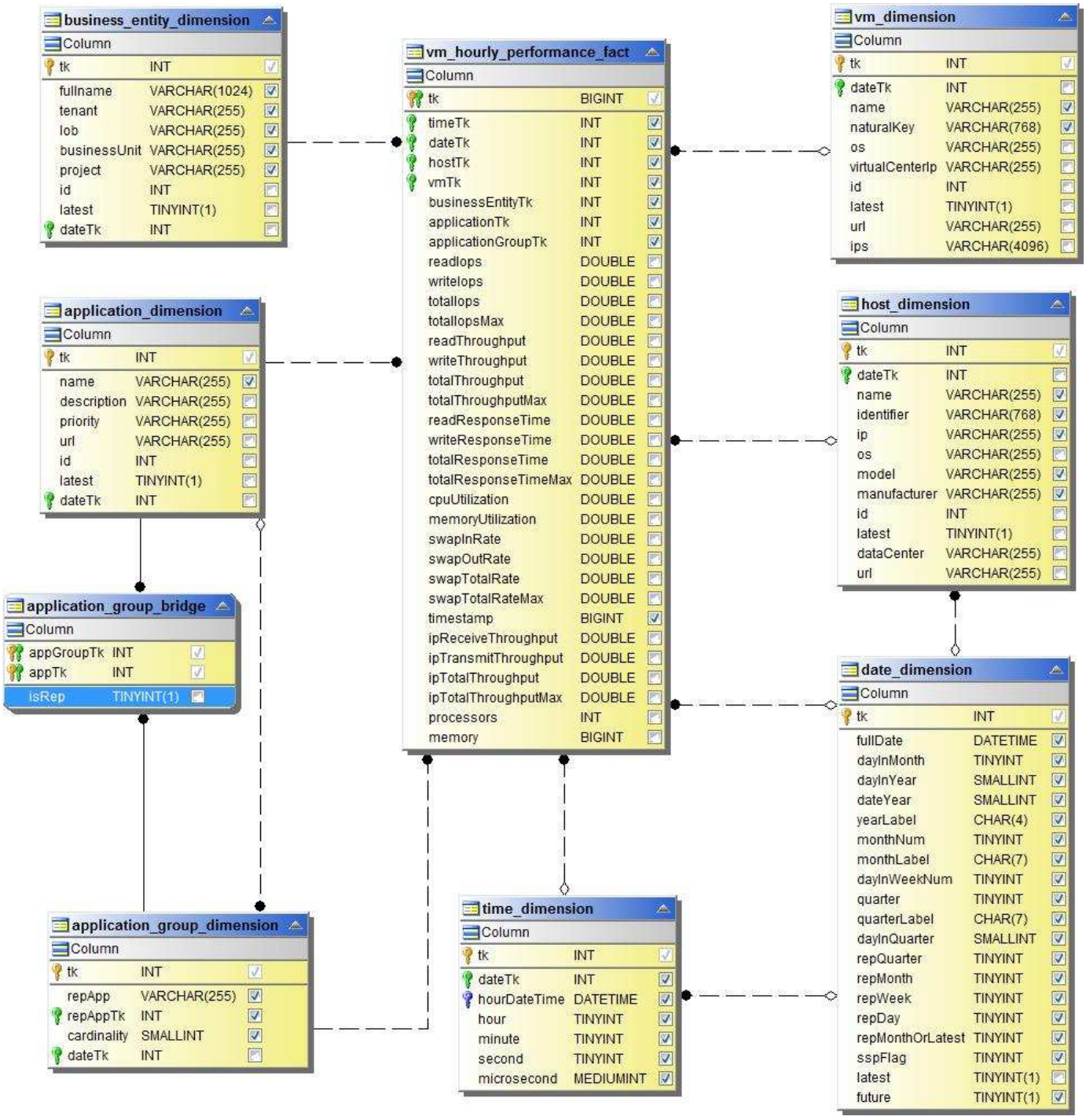
Prestazioni orarie della VM per l'host



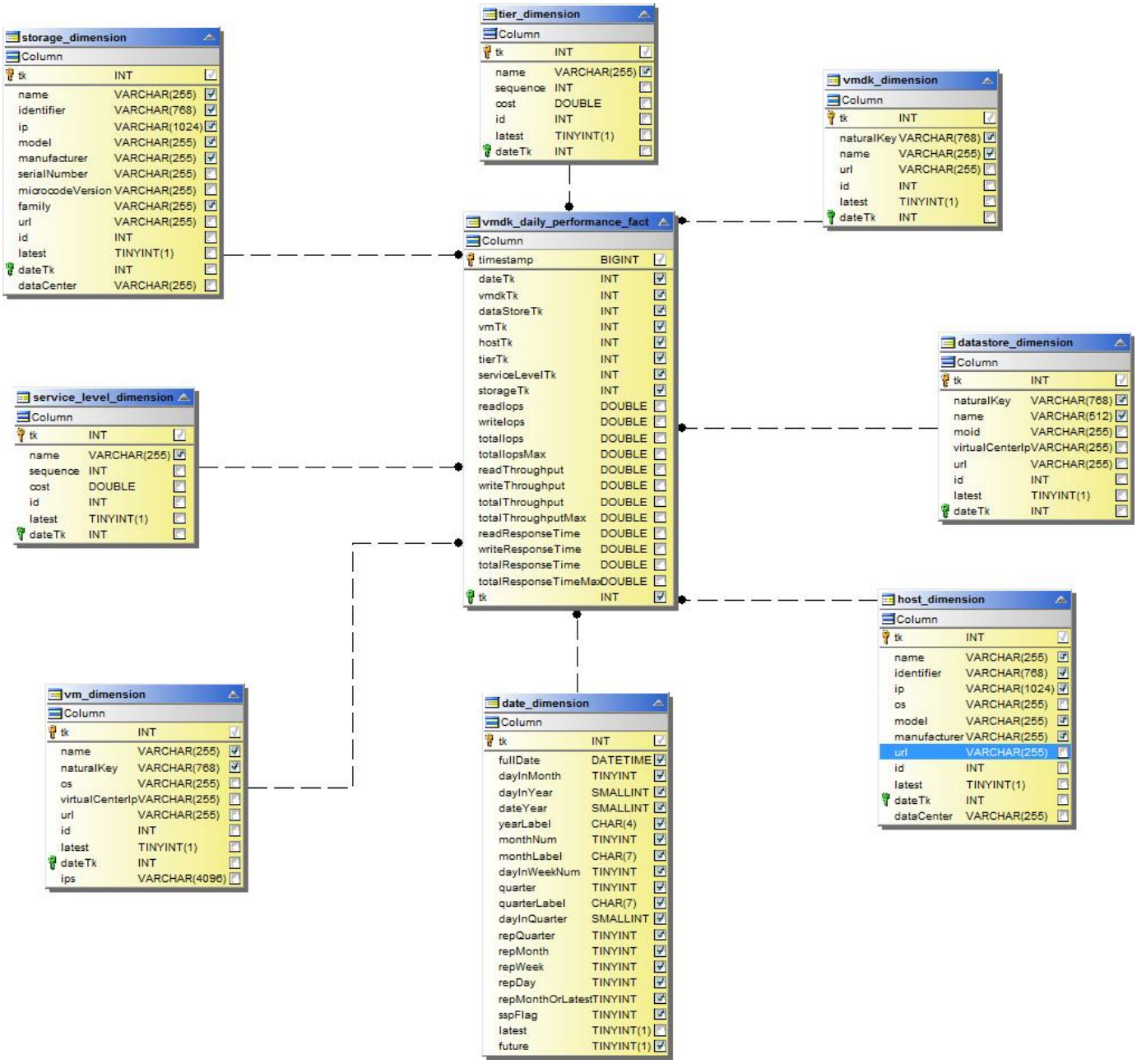
Prestazioni giornaliere della VM per l'host



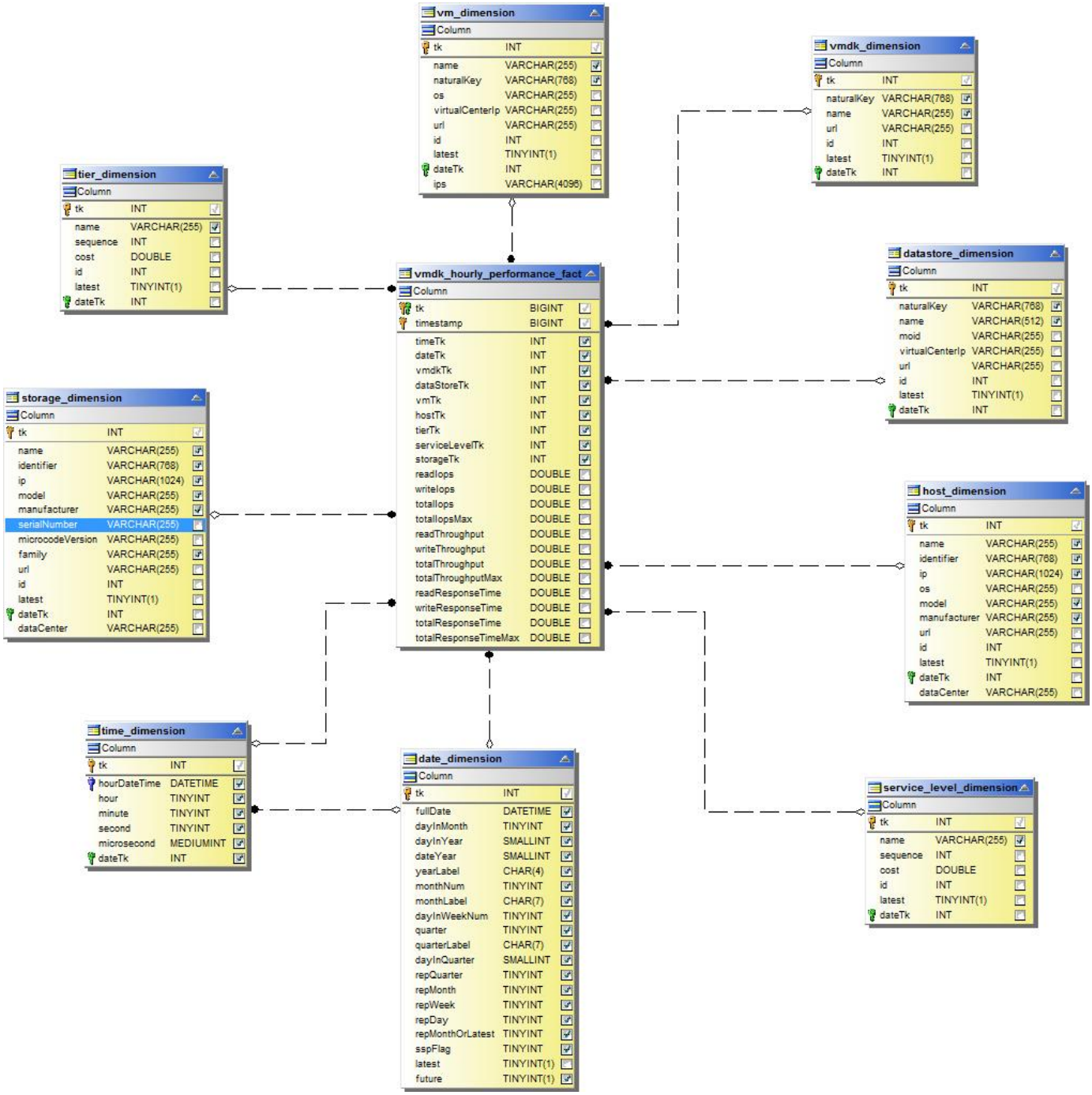
Prestazioni orarie della VM per l'host



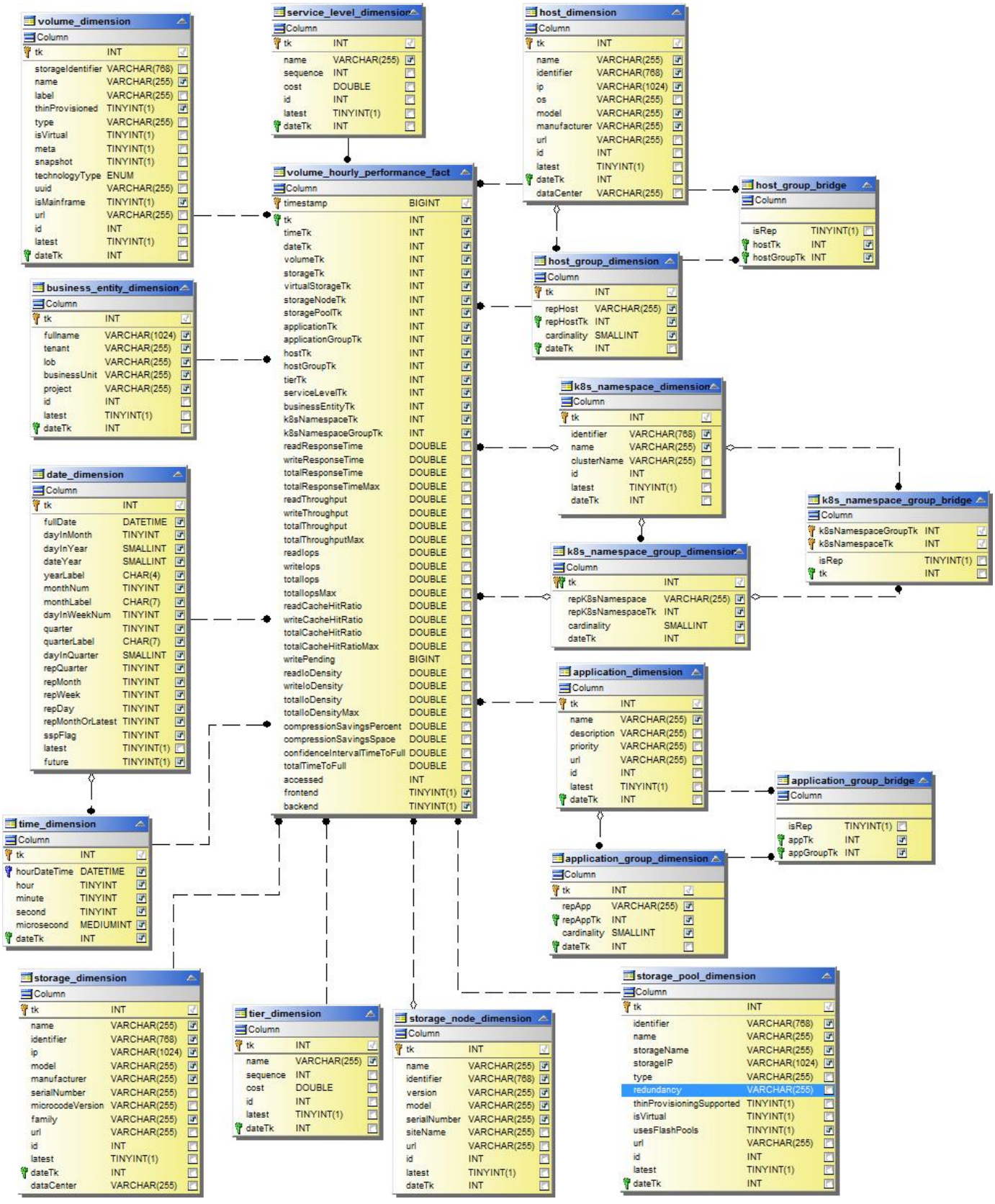
Prestazioni giornaliere VMDK



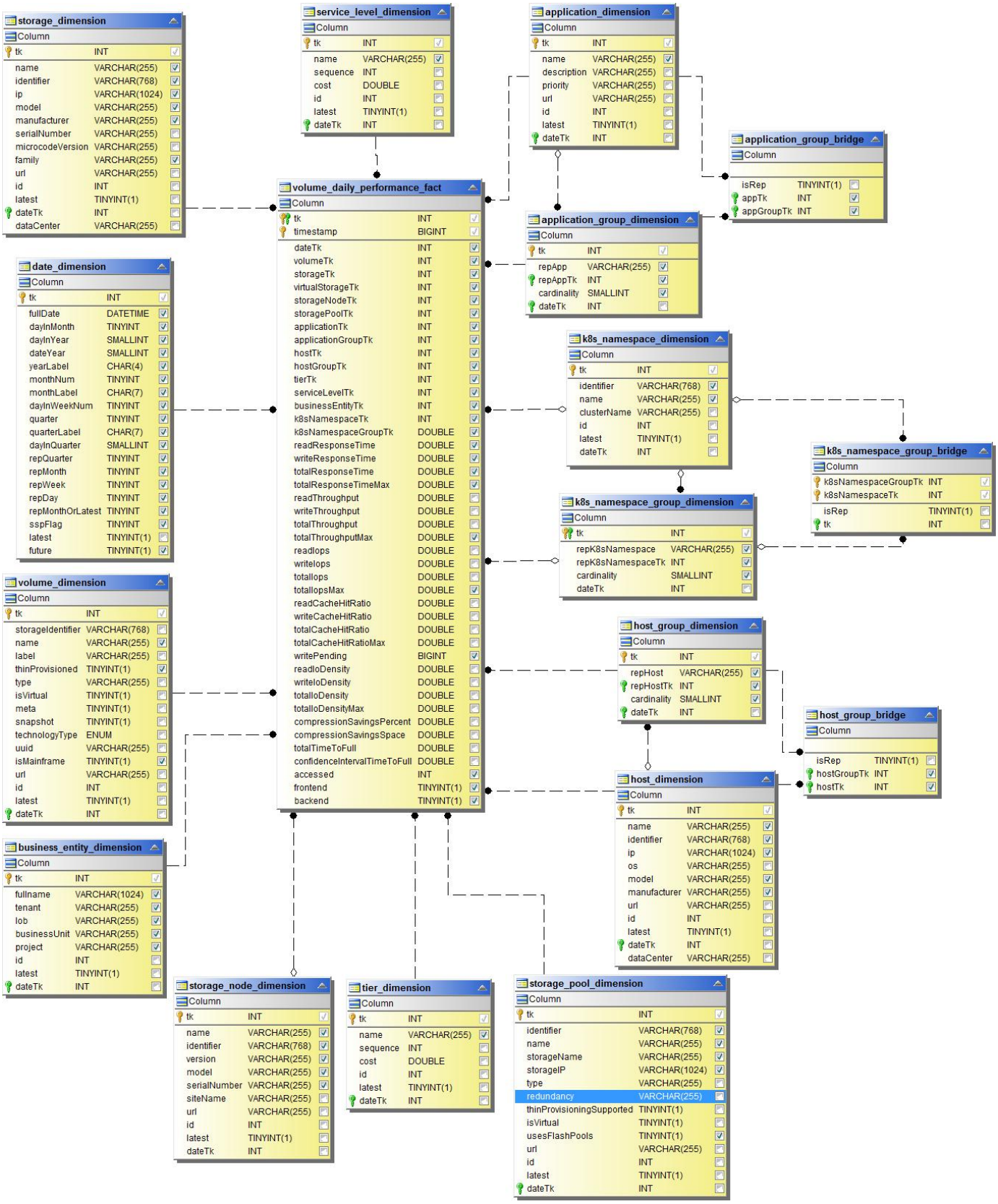
Prestazioni orarie VMDK



Prestazioni orarie del volume



Volume delle prestazioni giornaliere



Schemi Data Infrastructure Insights per la creazione di report

Queste tabelle e diagrammi di schema vengono forniti qui come riferimento per Data Infrastructure Insights Reporting.

"Tabelle degli schemi"in formato .PDF. Fare clic sul collegamento per aprirlo oppure fare clic con il pulsante destro del mouse e scegliere *Salva con nome…* per scaricarlo.

"Diagrammi di schema"

La funzionalità di reporting è disponibile in Data Infrastructure Insights"Edizione Premium" .

Kubernetes

Panoramica del cluster Kubernetes

Data Infrastructure Insights Kubernetes Explorer è un potente strumento per visualizzare lo stato generale e l'utilizzo dei cluster Kubernetes e consente di analizzare in modo più approfondito le aree di indagine.

Facendo clic su **Dashboard > Kubernetes Explorer** si apre la pagina con l'elenco dei cluster Kubernetes. Questa pagina di panoramica contiene la tabella dei cluster Kubernetes presenti nel tuo tenant.

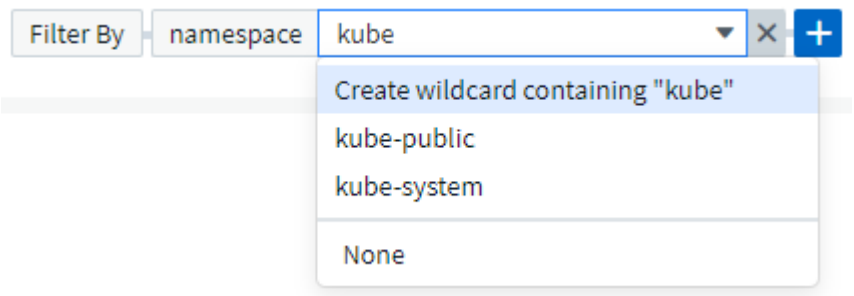
Elenco dei cluster

L'elenco dei cluster visualizza le seguenti informazioni per ciascun cluster nel tenant:

- Cluster **Nome**. Facendo clic sul nome di un cluster si aprirà il"**pagina dei dettagli**" per quel cluster.
- Percentuali di **saturazione**. La saturazione complessiva è la più alta tra la saturazione della CPU, della memoria o dello storage.
- Numero di **Nodi** nel cluster. Facendo clic su questo numero si aprirà la pagina dell'elenco dei nodi.
- Numero di **Pod** nel cluster. Facendo clic su questo numero si aprirà la pagina dell'elenco dei Pod.
- Numero di **Namespace** nel cluster. Facendo clic su questo numero si aprirà la pagina dell'elenco degli spazi dei nomi.
- Numero di **carichi di lavoro** nel cluster. Facendo clic su questo numero si aprirà la pagina dell'elenco dei carichi di lavoro.

Perfezionamento del filtro

Quando si filtra, quando si inizia a digitare viene presentata l'opzione per creare un **filtro con caratteri jolly** in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione jolly. È anche possibile creare **espressioni** utilizzando NOT o AND, oppure selezionare l'opzione "Nessuno" per filtrare i valori nulli nel campo.



I filtri basati su caratteri jolly o espressioni (ad esempio NOT, AND, "Nessuno", ecc.) vengono visualizzati in blu scuro nel campo filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in azzurro.

I filtri di Kubernetes sono contestuali, il che significa che se ci si trova, ad esempio, su una pagina di un nodo specifico, il filtro pod_name elenca solo i pod correlati a quel nodo. Inoltre, se si applica un filtro per uno specifico namespace, il filtro pod_name elencherà solo i pod su quel nodo *e* in quello namespace.

Si noti che il filtro con caratteri jolly ed espressioni funziona con testo o elenchi, ma non con valori numerici, date o valori booleani.

Prima di installare o aggiornare NetApp Kubernetes Monitoring Operator

Leggere queste informazioni prima di installare o aggiornare il"Operatore di monitoraggio Kubernetes" .

Componente	Requisito
Versione di Kubernetes	Kubernetes v1.20 e versioni successive.
Distribuzioni Kubernetes	AWS Elastic Kubernetes Service (EKS) Azure Kubernetes Service (AKS) Google Kubernetes Engine (GKE) Red Hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu
Sistema operativo Linux	Data Infrastructure Insights non supporta i nodi in esecuzione con architettura Arm64. Monitoraggio di rete: è necessario eseguire il kernel Linux versione 4.18.0 o successiva. Photon OS non è supportato.
Etichette	Data Infrastructure Insights supporta il monitoraggio dei nodi Kubernetes che eseguono Linux, specificando un selettore di nodi Kubernetes che cerca le seguenti etichette Kubernetes su queste piattaforme: Kubernetes v1.20 e versioni successive: Kubernetes.io/os = linux Rancher + cattle.io come piattaforma di orchestrazione/Kubernetes: cattle.io/os = linux
Comandi	I comandi curl e kubectl devono essere disponibili; per risultati ottimali, aggiungili al PATH.

Componente	Requisito
Connettività	kubectl cli è configurato per comunicare con il cluster K8s di destinazione e per avere connettività Internet con l'ambiente Data Infrastructure Insights . Se durante l'installazione ci si trova dietro un proxy, seguire le istruzioni riportate nel"Configurazione del supporto proxy" sezione dell'installazione dell'operatore. Per un audit e una segnalazione dei dati accurati, sincronizzare l'ora sulla macchina dell'agente utilizzando il protocollo NTP (Network Time Protocol) o il protocollo SNTP (Simple Network Time Protocol).
Altro	Se utilizzi OpenShift 4.6 o versione successiva, devi seguire le istruzioni"Istruzioni OpenShift" oltre a garantire che questi prerequisiti siano soddisfatti.
Token API	Se si sta ridistribuendo l'operatore (ovvero lo si sta aggiornando o sostituendo), non è necessario creare un nuovo token API; è possibile riutilizzare il token precedente.

Cose importanti da notare prima di iniziare

Se stai correndo con unprocuratore , avere unrepository personalizzato , o stanno usandoOpenShift , leggere attentamente le seguenti sezioni.

Leggi anche suPermessi .

Configurazione del supporto proxy

Esistono due posizioni in cui è possibile utilizzare un proxy sul tenant per installare NetApp Kubernetes Monitoring Operator. Possono essere gli stessi sistemi proxy o sistemi proxy separati:

- Proxy necessario durante l'esecuzione dello snippet di codice di installazione (utilizzando "curl") per connettere il sistema in cui viene eseguito lo snippet al tuo ambiente Data Infrastructure Insights
- Proxy necessario al cluster Kubernetes di destinazione per comunicare con l'ambiente Data Infrastructure Insights

Se si utilizza un proxy per uno o entrambi questi elementi, per installare NetApp Kubernetes Operating Monitor è necessario innanzitutto assicurarsi che il proxy sia configurato per consentire una buona comunicazione con l'ambiente Data Infrastructure Insights . Ad esempio, dai server/VM da cui si desidera installare l'operatore, è necessario poter accedere a Data Infrastructure Insights e poter scaricare i file binari da Data Infrastructure Insights.

Per il proxy utilizzato per installare NetApp Kubernetes Operating Monitor, prima di installare l'operatore, impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare anche la variabile di ambiente *no_proxy*.

Per impostare le variabili, eseguire i seguenti passaggi sul sistema **prima** di installare NetApp Kubernetes Monitoring Operator:

1. Imposta le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:

a. Se il proxy da configurare non dispone di autenticazione (nome utente/password), eseguire il seguente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Se il proxy da configurare dispone di autenticazione (nome
utente/password), eseguire questo comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Per far sì che il proxy utilizzato per il cluster Kubernetes comunichi con l'ambiente Data Infrastructure Insights , installare NetApp Kubernetes Monitoring Operator dopo aver letto tutte queste istruzioni.

Configurare la sezione proxy di AgentConfiguration in operator-config.yaml prima di distribuire NetApp Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utilizzo di un repository Docker personalizzato o privato

Per impostazione predefinita, NetApp Kubernetes Monitoring Operator estrarrà le immagini dei container dal repository Data Infrastructure Insights . Se si utilizza un cluster Kubernetes come destinazione per il monitoraggio e tale cluster è configurato per estrarre immagini di container solo da un repository Docker personalizzato o privato o da un registro di container, è necessario configurare l'accesso ai container necessari all'operatore di monitoraggio NetApp Kubernetes.

Eseguire "Image Pull Snippet" dal riquadro di installazione di NetApp Monitoring Operator. Questo comando effettuerà l'accesso al repository Data Infrastructure Insights , estrarrà tutte le dipendenze delle immagini per l'operatore e uscirà dal repository Data Infrastructure Insights . Quando richiesto, immettere la password temporanea del repository fornita. Questo comando scarica tutte le immagini utilizzate dall'operatore, comprese quelle per le funzionalità opzionali. Di seguito sono riportate le funzioni per cui vengono utilizzate queste immagini.

Funzionalità dell'operatore principale e monitoraggio di Kubernetes

- monitoraggio netapp
- kube-rbac-proxy
- metriche dello stato di Kube
- telegrafo
- utente root senza distribuzione

Registro eventi

- fluente-bit
- esportatore di eventi kubernetes

Prestazioni e mappa della rete

- ci-net-observer

Invia l'immagine Docker dell'operatore al tuo repository Docker privato/locale/aziendale in base alle policy aziendali. Assicurati che i tag delle immagini e i percorsi delle directory di queste immagini nel tuo repository siano coerenti con quelli nel repository Data Infrastructure Insights .

Modifica la distribuzione monitoring-operator in operator-deployment.yaml e modifica tutti i riferimenti alle immagini per utilizzare il tuo repository Docker privato.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modifica AgentConfiguration in operator-config.yaml per riflettere la nuova posizione del repository Docker. Crea un nuovo imagePullSecret per il tuo repository privato, per maggiori dettagli consulta *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation for
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository[using a custom or private docker repository].
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Istruzioni OpenShift

Se utilizzi OpenShift 4.6 o versione successiva, devi modificare AgentConfiguration in *operator-config.yaml* per abilitare l'impostazione *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift potrebbe implementare un livello di sicurezza aggiuntivo che potrebbe bloccare l'accesso ad alcuni componenti di Kubernetes.

Permessi

Se il cluster che stai monitorando contiene risorse personalizzate che non hanno un ClusterRole che"aggregati da visualizzare" , sarà necessario concedere manualmente all'operatore l'accesso a queste risorse per monitorarle con i registri eventi.

1. Modificare *operator-additional-permissions.yaml* prima dell'installazione oppure, dopo l'installazione, modificare la risorsa *ClusterRole/<namespace>-additional-permissions*
2. Crea una nuova regola per gli apiGroup e le risorse desiderati con i verbi ["get", "watch", "list"]. Vedi \ https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. Applica le modifiche al cluster

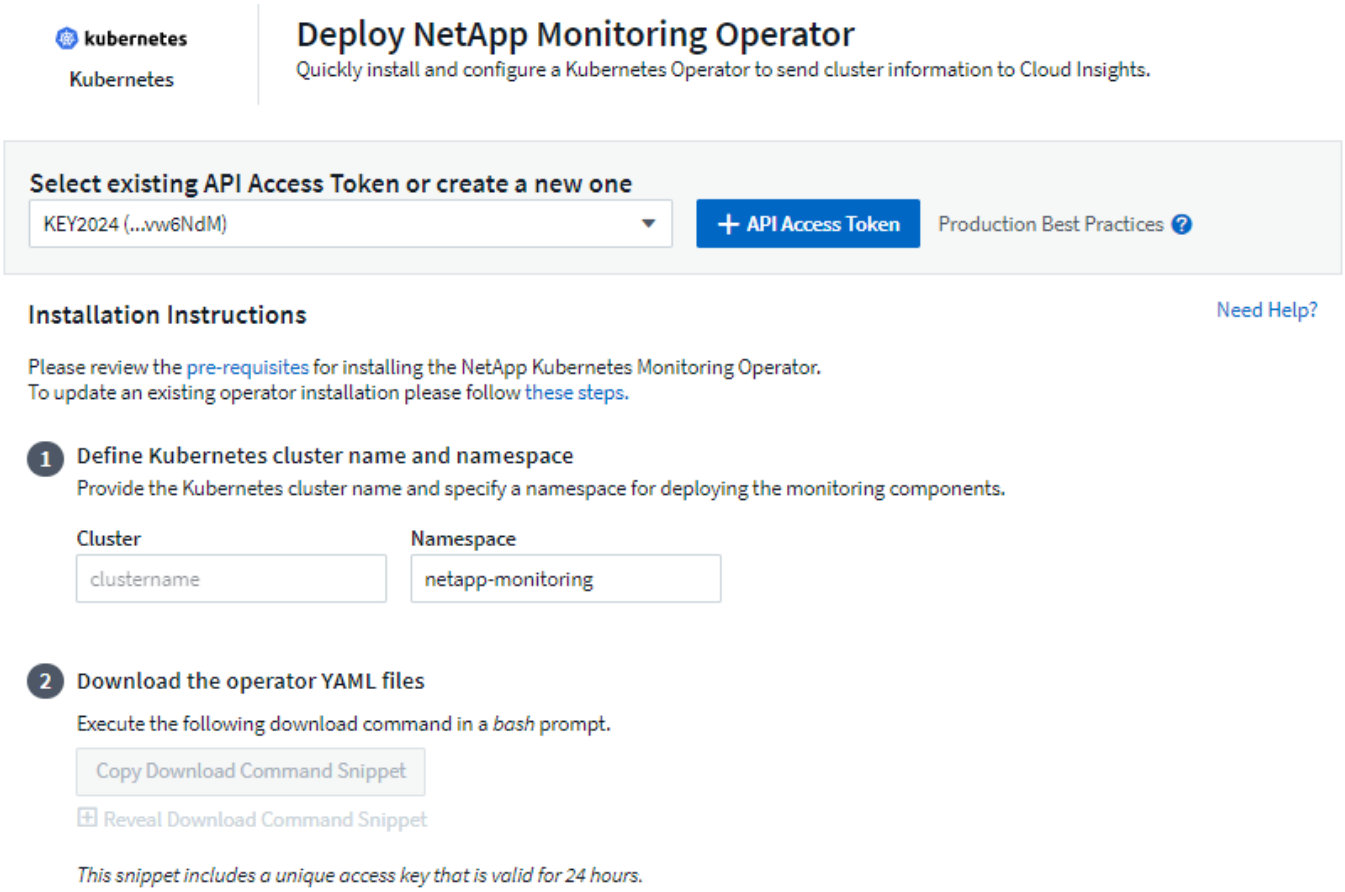
Installazione e configurazione dell'operatore di monitoraggio Kubernetes

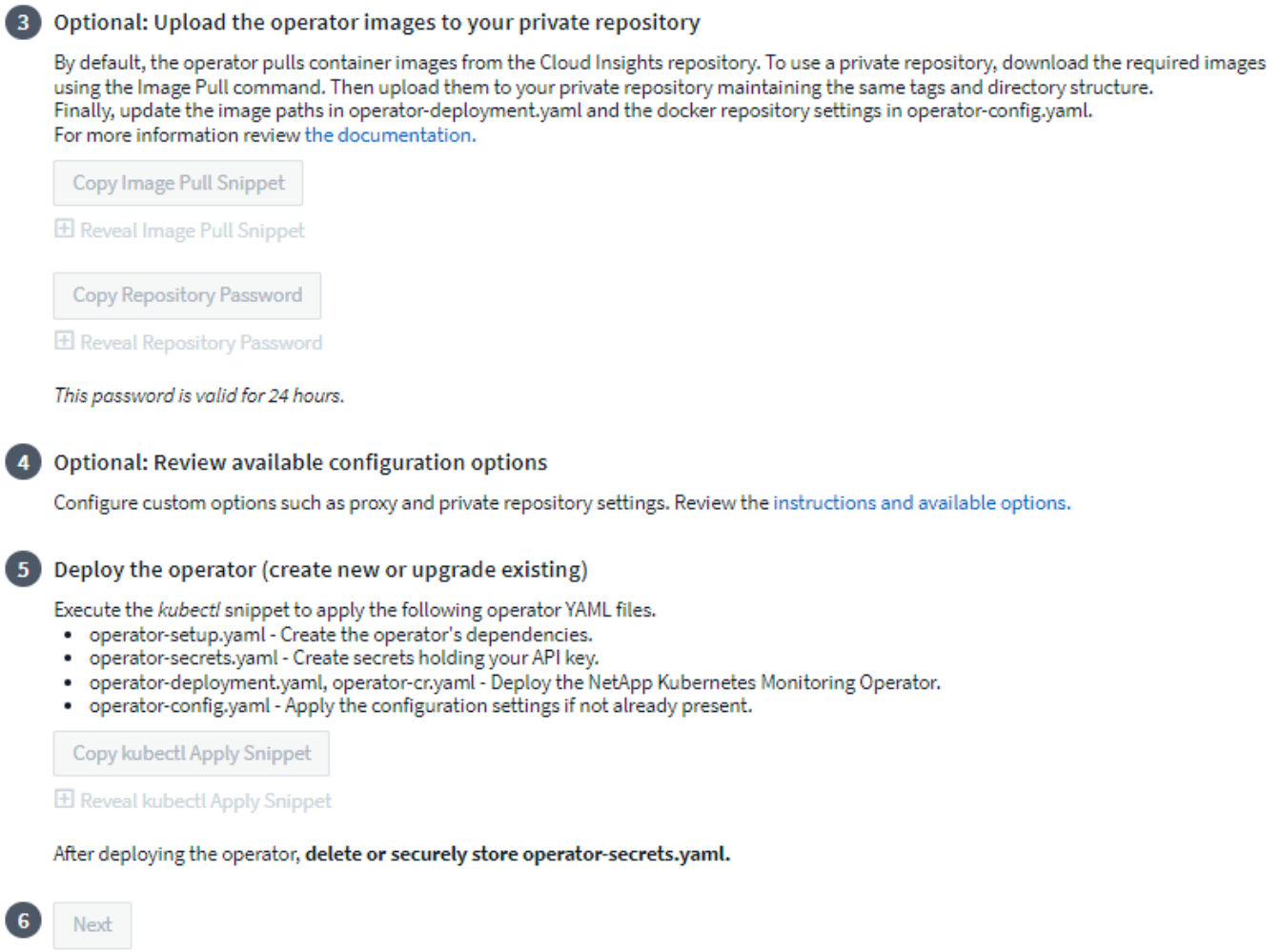
Data Infrastructure Insights offre l'**operatore di monitoraggio Kubernetes** per la raccolta Kubernetes. Passare a **Kubernetes > Collectors > +Kubernetes Collector** per distribuire un nuovo operatore.

Prima di installare Kubernetes Monitoring Operator

Vedi il"Prerequisiti" documentazione prima di installare o aggiornare Kubernetes Monitoring Operator.

Installazione dell'operatore di monitoraggio Kubernetes





Passaggi per installare l'agente Kubernetes Monitoring Operator su Kubernetes:

1. Immettere un nome cluster e uno spazio dei nomi univoci. Se seiaggiornamento da un precedente operatore Kubernetes, utilizzare lo stesso nome del cluster e lo stesso spazio dei nomi.
2. Una volta inseriti questi dati, è possibile copiare il frammento del comando Download negli appunti.
3. Incolla lo snippet in una finestra *bash* ed eseguilo. Verranno scaricati i file di installazione dell'operatore. Si noti che lo snippet ha una chiave univoca ed è valido per 24 ore.
4. Se hai un repository personalizzato o privato, copia il frammento di codice Image Pull facoltativo, incollalo in una shell *bash* ed eseguilo. Una volta estratte le immagini, copiale nel tuo repository privato. Assicuratevi di mantenere gli stessi tag e la stessa struttura delle cartelle. Aggiornare i percorsi in *operator-deployment.yaml* e le impostazioni del repository Docker in *operator-config.yaml*.
5. Se lo si desidera, rivedere le opzioni di configurazione disponibili, come le impostazioni del proxy o del repository privato. Puoi leggere di più su"opzioni di configurazione" .
6. Quando sei pronto, distribuisci l'operatore copiando lo snippet Apply di kubectl, scaricandolo ed eseguendolo.
7. L'installazione procede automaticamente. Una volta completato, fare clic sul pulsante *Avanti*.
8. Al termine dell'installazione, fare clic sul pulsante *Avanti*. Assicurati di eliminare o archiviare in modo sicuro anche il file *operator-secrets.yaml*.

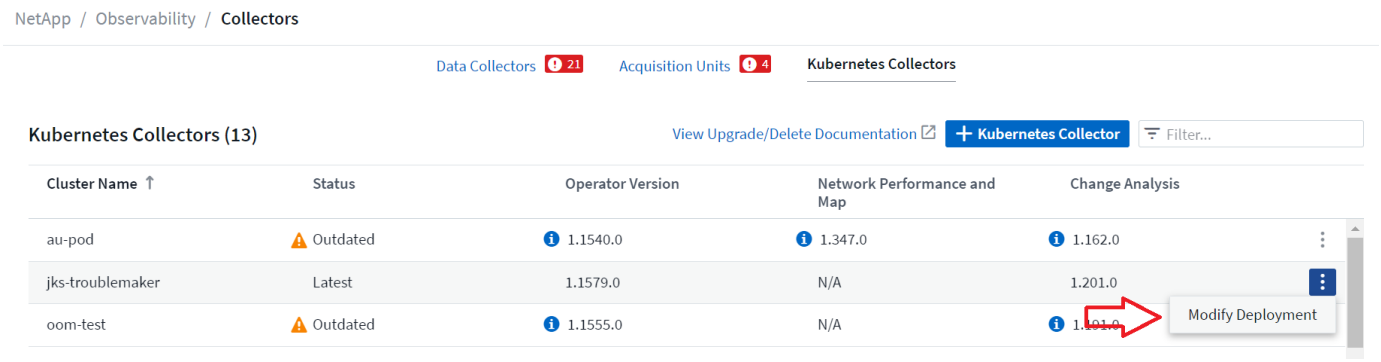
Se hai un repository personalizzato, leggi a riguardoutilizzando un repository Docker personalizzato/privato .

Componenti di monitoraggio di Kubernetes

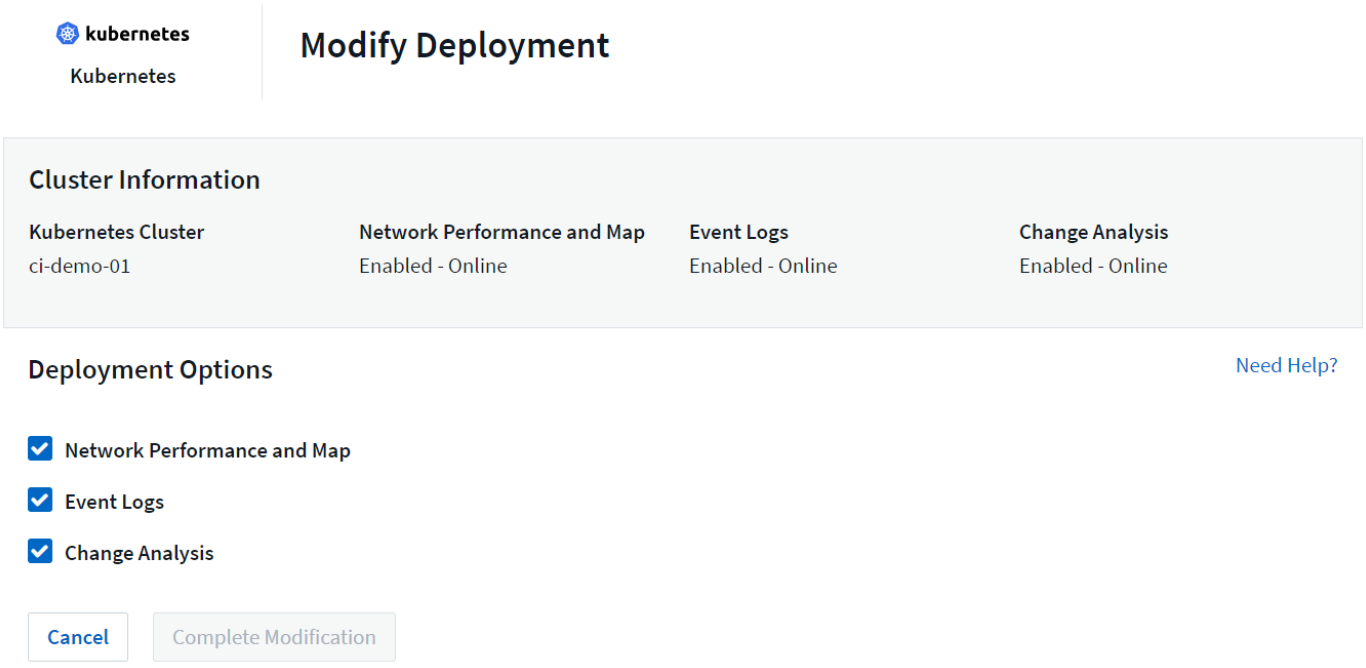
Data Infrastructure Insights Kubernetes Monitoring è composto da quattro componenti di monitoraggio:

- Metriche del cluster
- Prestazioni di rete e mappa (facoltativo)
- Registri eventi (facoltativo)
- Analisi del cambiamento (facoltativo)

I componenti facoltativi sopra indicati sono abilitati per impostazione predefinita per ciascun collector Kubernetes; se decidi che non hai bisogno di un componente per un collector specifico, puoi disabilitarlo andando su **Kubernetes > Collectors** e selezionando *Modifica distribuzione* dal menu "tre punti" del collector sulla destra dello schermo.



La schermata mostra lo stato attuale di ciascun componente e consente di disabilitare o abilitare i componenti per quel raccoglitore, a seconda delle necessità.



Aggiornamento all'ultima versione di Kubernetes Monitoring Operator

Aggiornamenti dei pulsanti DII

È possibile aggiornare Kubernetes Monitoring Operator tramite la pagina DII Kubernetes Collectors. Fare clic sul menu accanto al cluster che si desidera aggiornare e selezionare *Aggiorna*. L'operatore verificherà le firme delle immagini, eseguirà uno snapshot dell'installazione corrente ed eseguirà l'aggiornamento. Entro pochi minuti dovresti vedere l'avanzamento dello Stato dell'operatore da Aggiornamento in corso a Ultimo. Se si verifica un errore, è possibile selezionare lo stato Errore per maggiori dettagli e fare riferimento alla tabella di risoluzione dei problemi degli aggiornamenti tramite pulsante riportata di seguito.

Aggiornamenti rapidi con repository privati

Se il tuo operatore è configurato per utilizzare un repository privato, assicurati che tutte le immagini necessarie per eseguire l'operatore e le relative firme siano disponibili nel tuo repository. Se durante il processo di aggiornamento si verifica un errore per immagini mancanti, è sufficiente aggiungerle al repository e riprovare l'aggiornamento. Per caricare le firme delle immagini nel tuo repository, utilizza lo strumento di co-firma come segue, assicurandoti di caricare le firme per tutte le immagini specificate in 3 Facoltativo: carica le immagini dell'operatore nel tuo repository privato > Frammento di estrazione dell'immagine

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Ripristino di una versione precedentemente in esecuzione

Se hai effettuato l'aggiornamento utilizzando la funzionalità di aggiornamento tramite pulsante e riscontri difficoltà con la versione corrente dell'operatore entro sette giorni dall'aggiornamento, puoi effettuare il downgrade alla versione in esecuzione in precedenza utilizzando lo snapshot creato durante il processo di aggiornamento. Fare clic sul menu accanto al cluster di cui si desidera eseguire il rollback e selezionare *Roll back*.

Aggiornamenti manuali

Determinare se esiste un *AgentConfiguration* con l'operatore esistente (se il namespace non è il *netapp-monitoring* predefinito, sostituire il namespace appropriato):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Se esiste un _AgentConfiguration_:
```

- Installarel'ultimo Operatore rispetto all'Operatore esistente.
  - Assicurati di essereestrazione delle ultime immagini del contenitore se si utilizza un repository personalizzato.

Se *AgentConfiguration* non esiste:

- Prendi nota del nome del tuo cluster riconosciuto da Data Infrastructure Insights (se il tuo namespace non è quello predefinito netapp-monitoring, sostituiscilo con il namespace appropriato):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Crea un backup dell'operatore esistente (se il tuo namespace non è il
netapp-monitoring predefinito, sostituiscilo con il namespace
appropriato):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-
operator,Disinstallare>>l'operatore esistente.
* <<installing-the-kubernetes-monitoring-operator,Installare>>l'ultimo
Operatore.
```

- Utilizzare lo stesso nome del cluster.
- Dopo aver scaricato gli ultimi file YAML dell'Operator, trasferisci tutte le personalizzazioni trovate in *agent_backup.yaml* nel *operator-config.yaml* scaricato prima della distribuzione.
- Assicurati di essereestrazione delle ultime immagini del contenitore se si utilizza un repository personalizzato.

Arresto e avvio dell'operatore di monitoraggio Kubernetes

Per arrestare Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Per avviare Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Disinstallazione

Per rimuovere l'operatore di monitoraggio Kubernetes

Si noti che lo spazio dei nomi predefinito per l'operatore di monitoraggio Kubernetes è "netapp-monitoring". Se hai impostato un tuo namespace, sostituiscilo in questi e in tutti i comandi e file successivi.

Le versioni più recenti dell'operatore di monitoraggio possono essere disinstallate con i seguenti comandi:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Se l'operatore di monitoraggio è stato distribuito nel proprio namespace dedicato, eliminare il namespace:

```
 kubectl delete ns <NAMESPACE>
Nota: se il primo comando restituisce "Nessuna risorsa trovata",
utilizzare le seguenti istruzioni per disinstallare le versioni precedenti
dell'operatore di monitoraggio.
```

Eseguire ciascuno dei seguenti comandi nell'ordine indicato. A seconda dell'installazione corrente, alcuni di questi comandi potrebbero restituire messaggi di tipo "oggetto non trovato". Questi messaggi possono essere tranquillamente ignorati.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Se in precedenza è stato creato un vincolo di contesto di sicurezza:

```
kubectl delete scc telegraf-hostaccess
```

Informazioni su Kube-state-metrics

NetApp Kubernetes Monitoring Operator installa le proprie metriche kube-state per evitare conflitti con altre istanze.

Per informazioni su Kube-State-Metrics, vedere"questa pagina" .

Configurazione/Personalizzazione dell'operatore

Queste sezioni contengono informazioni sulla personalizzazione della configurazione dell'operatore, sull'utilizzo del proxy, sull'utilizzo di un repository Docker personalizzato o privato o sull'utilizzo di OpenShift.

Opzioni di configurazione

Le impostazioni modificate più comunemente possono essere configurate nella risorsa personalizzata *AgentConfiguration*. È possibile modificare questa risorsa prima di distribuire l'operatore modificando il file *operator-config.yaml*. Questo file include esempi di impostazioni commentati. Vedi l'elenco di"impostazioni disponibili" per la versione più recente dell'operatore.

È anche possibile modificare questa risorsa dopo aver distribuito l'operatore utilizzando il seguente comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Per determinare se la versione distribuita dell'operatore supporta
_AgentConfiguration_, eseguire il seguente comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se viene visualizzato il messaggio "Errore dal server (NotFound)", è
necessario aggiornare l'operatore prima di poter utilizzare
AgentConfiguration.
```

Configurazione del supporto proxy

Esistono due posti in cui è possibile utilizzare un proxy sul tenant per installare Kubernetes Monitoring Operator. Possono essere gli stessi sistemi proxy o sistemi proxy separati:

- Proxy necessario durante l'esecuzione dello snippet di codice di installazione (utilizzando "curl") per connettere il sistema in cui viene eseguito lo snippet al tuo ambiente Data Infrastructure Insights
- Proxy necessario al cluster Kubernetes di destinazione per comunicare con l'ambiente Data Infrastructure Insights

Se si utilizza un proxy per uno o entrambi questi elementi, per installare Kubernetes Operating Monitor è necessario innanzitutto assicurarsi che il proxy sia configurato per consentire una buona comunicazione con l'ambiente Data Infrastructure Insights . Se disponi di un proxy e puoi accedere a Data Infrastructure Insights dal server/VM da cui desideri installare l'operatore, è probabile che il tuo proxy sia configurato correttamente.

Per il proxy utilizzato per installare Kubernetes Operating Monitor, prima di installare l'operatore, impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare anche la variabile di ambiente *no_proxy*.

Per impostare le variabili, esegui i seguenti passaggi sul tuo sistema **prima** di installare Kubernetes Monitoring Operator:

1. Imposta le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:
   a. Se il proxy da configurare non dispone di autenticazione (nome utente/password), eseguire il seguente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Se il proxy da configurare dispone di autenticazione (nome
utente/password), eseguire questo comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Per far sì che il proxy utilizzato per il cluster Kubernetes comunichi con l'ambiente Data Infrastructure Insights , installare Kubernetes Monitoring Operator dopo aver letto tutte queste istruzioni.

Configura la sezione proxy di *AgentConfiguration* in *operator-config.yaml* prima di distribuire Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utilizzo di un repository Docker personalizzato o privato

Per impostazione predefinita, Kubernetes Monitoring Operator estrarrà le immagini dei container dal repository Data Infrastructure Insights . Se si utilizza un cluster Kubernetes come destinazione per il monitoraggio e tale cluster è configurato per estrarre immagini di container solo da un repository Docker personalizzato o privato o da un registro di container, è necessario configurare l'accesso ai container necessari all'operatore di monitoraggio Kubernetes.

Eseguire "Image Pull Snippet" dal riquadro di installazione di NetApp Monitoring Operator. Questo comando effettuerà l'accesso al repository Data Infrastructure Insights , estrarrà tutte le dipendenze delle immagini per l'operatore e uscirà dal repository Data Infrastructure Insights . Quando richiesto, immettere la password temporanea del repository fornita. Questo comando scarica tutte le immagini utilizzate dall'operatore, comprese quelle per le funzionalità opzionali. Di seguito sono riportate le funzioni per cui vengono utilizzate queste immagini.

Funzionalità dell'operatore principale e monitoraggio di Kubernetes

- monitoraggio netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf

- utente root senza distribuzione

Registro eventi

- ci-fluent-bit
- ci-kubernetes-event-exporter

Prestazioni e mappa della rete

- ci-net-observer

Invia l'immagine Docker dell'operatore al tuo repository Docker privato/locale/aziendale in base alle policy aziendali. Assicurati che i tag delle immagini e i percorsi delle directory di queste immagini nel tuo repository siano coerenti con quelli nel repository Data Infrastructure Insights .

Modifica la distribuzione monitoring-operator in operator-deployment.yaml e modifica tutti i riferimenti alle immagini per utilizzare il tuo repository Docker privato.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modifica *AgentConfiguration* in *operator-config.yaml* per riflettere la nuova posizione del docker repo. Crea un nuovo imagePullSecret per il tuo repository privato, per maggiori dettagli vedi *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Token di accesso API per password a lungo termine

Alcuni ambienti (ad esempio repository proxy) richiedono password a lungo termine per il Data Infrastructure Insights docker repository. La password fornita nell'interfaccia utente al momento dell'installazione è valida solo per 24 ore. Invece di utilizzare quella, si può usare un API Access Token come password del docker repository. Questa password sarà valida finché l'API Access Token sarà valido. Si può generare un nuovo API Access Token per questo scopo specifico o utilizzarne uno esistente.

"Leggi qui" per istruzioni su come creare un nuovo token di accesso API.

Per estrarre un API Access Token esistente da un file *operator-secrets.yaml* scaricato, gli utenti possono eseguire quanto segue:

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

Per estrarre un API Access Token esistente da un'installazione dell'operatore in esecuzione, gli utenti possono eseguire quanto segue:

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

Istruzioni OpenShift

Se si utilizza OpenShift 4.6 o versioni successive, è necessario modificare *AgentConfiguration* in *operator-config.yaml* per abilitare l'impostazione *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift potrebbe implementare un livello di sicurezza aggiuntivo che potrebbe bloccare l'accesso ad alcuni componenti di Kubernetes.

Tolleranze e difetti

I DaemonSet *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* e *netapp-ci-net-observer-l4-ds* devono pianificare un pod su ogni nodo del cluster per raccogliere correttamente i dati su tutti i nodi. L'operatore è stato configurato per tollerare alcune **imperfezioni** ben note. Se hai configurato delle taint personalizzate sui tuoi nodi, impedendo così ai pod di essere eseguiti su ogni nodo, puoi creare una **tolleranza** per quelle taint"nella *AgentConfiguration*" . Se hai applicato taint personalizzati a tutti i nodi del tuo cluster, devi anche aggiungere le tolleranze necessarie alla distribuzione dell'operatore per consentire la pianificazione e l'esecuzione del pod dell'operatore.

Scopri di più su Kubernetes"Contaminazioni e tolleranze" .

Ritorno al"* Pagina di installazione dell'operatore di monitoraggio NetApp Kubernetes*"

Una nota sui segreti

Per rimuovere l'autorizzazione per l'operatore di monitoraggio Kubernetes a visualizzare i segreti a livello di cluster, eliminare le seguenti risorse dal file *operator-setup.yaml* prima dell'installazione:

```
ClusterRole/netapp-ci<namespace>-agent-secret
ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

Se si tratta di un aggiornamento, elimina anche le risorse dal tuo cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Se l'analisi delle modifiche è abilitata, modificare *AgentConfiguration* o *operator-config.yaml* per rimuovere il commento dalla sezione change-management e includere *kindsToIgnoreFromWatch: '"secrets"'* nella sezione change-management. Notare la presenza e la posizione delle virgolette singole e doppie in questa riga.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Verifica delle firme delle immagini degli operatori di monitoraggio di Kubernetes

L'immagine per l'operatore e tutte le immagini correlate che distribuisce sono firmate da NetApp. È possibile verificare manualmente le immagini prima dell'installazione utilizzando lo strumento di co-firma oppure configurare un controller di ammissione Kubernetes. Per maggiori dettagli si prega di consultare il"Documentazione di Kubernetes" .

La chiave pubblica utilizzata per verificare le firme delle immagini è disponibile nel riquadro di installazione dell'operatore di monitoraggio in *Facoltativo: carica le immagini dell'operatore nel tuo repository privato > Chiave pubblica della firma dell'immagine*

Per verificare manualmente una firma immagine, procedere come segue:

1. Copia ed esegui l'Image Pull Snippet
2. Copia e inserisci la password del repository quando richiesto
3. Memorizza la chiave pubblica della firma dell'immagine (dii-image-signing.pub nell'esempio)
4. Verificare le immagini tramite co-firma. Fare riferimento al seguente esempio di utilizzo del cosign

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi durante la configurazione dell'operatore di monitoraggio Kubernetes:

Problema:	Prova questo:
Non vedo alcun collegamento ipertestuale/connessione tra il mio volume persistente Kubernetes e il dispositivo di archiviazione back-end corrispondente. Il mio volume persistente Kubernetes è configurato utilizzando il nome host del server di archiviazione.	Seguire i passaggi per disinstallare l'agente Telegraf esistente, quindi reinstallare l'agente Telegraf più recente. È necessario utilizzare Telegraf versione 2.0 o successiva e l'archiviazione del cluster Kubernetes deve essere monitorata attivamente da Data Infrastructure Insights.

Problema:	Prova questo:
Nei log vedo messaggi simili ai seguenti: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.MutatingWebhookConfiguration: il server non è riuscito a trovare la risorsa richiesta E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.Lease: il server non è riuscito a trovare la risorsa richiesta (ottenere leases.coordination.k8s.io) ecc.	Questi messaggi possono essere visualizzati se si esegue kube-state-metrics versione 2.0.0 o successiva con versioni di Kubernetes precedenti alla 1.20. Per ottenere la versione di Kubernetes: *kubectl version* Per ottenere la versione di kube-state-metrics: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Per evitare che questi messaggi si verifichino, gli utenti possono modificare la distribuzione di kube-state-metrics per disabilitare i seguenti lease: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Più specificamente, possono utilizzare il seguente argomento CLI: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, secrets,services,statefulsets,storageclasses L’elenco di risorse predefinito è: "certificatesigningrequests,configmaps,cronjobs,daemonsets,deployments, endpoints,horizontalpodautoscalers,ingresses,jobs,leases,limitranges, mutatingwebhookconfigurations,namespaces,networkpolicies,nodes, persistentvolumeclaims,persistentvolumes,poddisruptionbudgets,pods,replicasets, replicationcontrollers,resourcequotas,secrets,services, statefulsets,storageclasses, validatingwebhookconfigurations,volumeattachments"

Problema:	Prova questo:
Vedo messaggi di errore da Telegraf simili ai seguenti, ma Telegraf si avvia ed è in esecuzione: 11 ott 14:23:41 ip-172-31-39-47 systemd[1]: Avviato L'agente server basato su plugin per la segnalazione delle metriche in InfluxDB. 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="impossibile creare la directory della cache. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: permesso negato. ignorato\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="apertura non riuscita. Ignorato. Apri /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: nessun file o directory\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z I! Avvio di Telegraf 1.19.3	Questo è un problema noto. Fare riferimento a"Questo articolo di GitHub" per maggiori dettagli. Finché Telegraf è attivo e funzionante, gli utenti possono ignorare questi messaggi di errore.
Su Kubernetes, i miei pod Telegraf segnalano il seguente errore: "Errore nell'elaborazione delle informazioni mountstats: impossibile aprire il file mountstats: /hostfs/proc/1/mountstats, errore: apertura /hostfs/proc/1/mountstats: autorizzazione negata"	Se SELinux è abilitato e applicato, è probabile che impedisca ai pod Telegraf di accedere al file /proc/1/mountstats sul nodo Kubernetes. Per superare questa restrizione, modificare agentconfiguration e abilitare l'impostazione runPrivileged. Per maggiori dettagli, fare riferimento alle istruzioni di OpenShift.
Su Kubernetes, il mio pod Telegraf ReplicaSet segnala il seguente errore: [inputs.prometheus] Errore nel plugin: impossibile caricare la coppia di chiavi /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: aprire /etc/kubernetes/pki/etcd/server.crt: nessun file o directory del genere	Il pod Telegraf ReplicaSet è progettato per essere eseguito su un nodo designato come master o per etcd. Se il pod ReplicaSet non è in esecuzione su uno di questi nodi, verranno visualizzati questi errori. Controlla se i tuoi nodi master/etcd presentano delle anomalie. In tal caso, aggiungere le tolleranze necessarie al Telegraf ReplicaSet, telegraf-rs. Ad esempio, modifica ReplicaSet… kubectl edit rs telegraf-rs …e aggiungi le tolleranze appropriate alla specifica. Quindi, riavviare il pod ReplicaSet.

Problema:	Prova questo:
Ho un ambiente PSP/PSA. Ciò ha ripercussioni sul mio operatore di monitoraggio?	Se il cluster Kubernetes è in esecuzione con Pod Security Policy (PSP) o Pod Security Admission (PSA), è necessario eseguire l'aggiornamento alla versione più recente di Kubernetes Monitoring Operator. Per effettuare l'aggiornamento all'operatore corrente con supporto per PSP/PSA, seguire questi passaggi: 1. Disinstallare l'operatore di monitoraggio precedente: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installare l'ultima versione dell'operatore di monitoraggio.
Ho riscontrato problemi nel tentativo di distribuire l'Operatore e sto utilizzando PSP/PSA.	1. Modificare l'agente utilizzando il seguente comando: kubectl -n <name-space> edit agent 2. Contrassegna 'security-policy-enabled' come 'false'. In questo modo verranno disattivati i criteri di sicurezza del Pod e l'ammissione di sicurezza del Pod e sarà consentito all'operatore di effettuare la distribuzione. Confermare utilizzando i seguenti comandi: kubectl get psp (dovrebbe mostrare che la politica di sicurezza del pod è stata rimossa) kubectl get all -n <namespace>
grep -i psp (dovrebbe mostrare che non è stato trovato nulla)	Errori "ImagePullBackoff" rilevati
Questi errori potrebbero verificarsi se si dispone di un repository Docker personalizzato o privato e non è ancora stato configurato Kubernetes Monitoring Operator per riconoscerlo correttamente. Per saperne di più sulla configurazione per repository personalizzati/privati.	Ho un problema con la distribuzione del mio operatore di monitoraggio e la documentazione attuale non mi aiuta a risolverlo.

Problema:	Prova questo:

Acquisire o annotare in altro modo l'output dei seguenti comandi e contattare il team di supporto tecnico.
 	
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all -containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all -containers=true`
	I pod net-observer (Workload Map) nello spazio dei nomi Operator sono in CrashLoopBackOff

Questi pod corrispondono al raccoglitore di dati Workload Map per Network Observability. Prova questi: • Controlla i log di uno dei pod per confermare la versione minima del kernel. Ad esempio: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"fallimento nella convalida. Motivo: la versione del kernel 3.10.0 è inferiore alla versione minima del kernel 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • I pod Net-observer richiedono che la versione del kernel Linux sia almeno 4.18.0. Controllare la versione del kernel utilizzando il comando "uname -r" e assicurarsi che sia >= 4.18.0	I pod sono in esecuzione nello spazio dei nomi Operatore (predefinito: netapp-monitoring), ma nell'interfaccia utente non vengono visualizzati dati per la mappa del carico di lavoro o metriche Kubernetes nelle query
Controllare l'impostazione dell'ora sui nodi del cluster K8S. Per un audit e una segnalazione dei dati accurati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'agente utilizzando il protocollo NTP (Network Time Protocol) o il protocollo SNTP (Simple Network Time Protocol).	Alcuni dei pod net-observer nello spazio dei nomi Operator sono nello stato In sospeso
Net-observer è un DaemonSet ed esegue un pod in ogni nodo del cluster k8s. • Prendi nota del pod che si trova nello stato In sospeso e controlla se sta riscontrando un problema di risorse per la CPU o la memoria. Assicurarsi che nel nodo siano disponibili la memoria e la CPU richieste.	Subito dopo aver installato Kubernetes Monitoring Operator, vedo quanto segue nei miei log: [inputs.prometheus] Errore nel plugin: errore durante la richiesta HTTP a http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Ottieni http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: dial tcp: cerca kube-state-metrics.<namespace>.svc.cluster.local: nessun host del genere

Problema:	Prova questo:
In genere questo messaggio viene visualizzato solo quando viene installato un nuovo operatore e il pod *telegraf-rs* è attivo prima del pod *ksm*. Questi messaggi dovrebbero cessare una volta che tutti i pod saranno in esecuzione.	Non vedo alcuna metrica raccolta per i CronJob di Kubernetes presenti nel mio cluster.
Verifica la tua versione di Kubernetes (ad esempio `kubectl version`). Se la versione è v1.20.x o precedente, si tratta di una limitazione prevista. La versione kube-state-metrics distribuita con Kubernetes Monitoring Operator supporta solo v1.CronJob. Con Kubernetes 1.20.x e versioni precedenti, la risorsa CronJob si trova in v1beta.CronJob. Di conseguenza, kube-state-metrics non riesce a trovare la risorsa CronJob.	Dopo aver installato l'operatore, i pod telegraf-ds entrano in CrashLoopBackOff e i log dei pod indicano "su: Authentication failure".
Modifica la sezione telegraf in *AgentConfiguration* e imposta *dockerMetricCollectionEnabled* su false. Per maggiori dettagli, fai riferimento a "opzioni di configurazione" dell'operatore. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Nei miei registri di Telegraf vedo messaggi di errore ricorrenti simili ai seguenti: E! [agente] Errore durante la scrittura su output.http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": scadenza del contesto superata (Client.Timeout superato durante l'attesa delle intestazioni)
Modificare la sezione telegraf in *AgentConfiguration* e aumentare *outputTimeout* a 10 s. Per maggiori dettagli fare riferimento al manuale dell'operatore"opzioni di configurazione" .	Mancano i dati *involvedobject* per alcuni registri eventi.
Assicurati di aver seguito i passaggi indicati in"Permessi" sezione sopra.	Perché vedo due pod di operatori di monitoraggio in esecuzione, uno denominato netapp-ci-monitoring-operator-<pod> e l'altro denominato monitoring-operator-<pod>?
A partire dal 12 ottobre 2023, Data Infrastructure Insights ha riorganizzato l'operatore per servire meglio i nostri utenti; affinché tali modifiche vengano adottate completamente, è necessariorimuovere il vecchio operatore Einstallare quello nuovo .	I miei eventi Kubernetes hanno smesso inaspettatamente di segnalare a Data Infrastructure Insights.
Recupera il nome del pod event-exporter: `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problema:	Prova questo:
awk '{print $1}'	sed 's/event-exporter./event-exporter/` Dovrebbe essere "netapp-ci-event-exporter" o "event-exporter". Successivamente, modifica l'agente di monitoraggio `kubectl -n netapp-monitoring edit agent` e impostare il valore per LOG_FILE in modo che rifletta il nome appropriato del pod di esportazione eventi trovato nel passaggio precedente. Più specificatamente, LOG_FILE dovrebbe essere impostato su "/var/log/containers/netapp-ci-event-exporter.log" o "/var/log/containers/event-exporter*.log" …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. In alternativa, si può anchedisinstallare Ereinstallare l'agente.
Vedo che i pod distribuiti dal Kubernetes Monitoring Operator si bloccano a causa di risorse insufficienti.	Fare riferimento all'operatore di monitoraggio Kubernetes"opzioni di configurazione" per aumentare i limiti della CPU e/o della memoria secondo necessità.
Un'immagine mancante o una configurazione non valida hanno impedito l'avvio o la disponibilità dei pod netapp-ci-kube-state-metrics. Ora StatefulSet è bloccato e le modifiche alla configurazione non vengono applicate ai pod netapp-ci-kube-state-metrics.	Lo StatefulSet è in un"rotto" stato. Dopo aver risolto eventuali problemi di configurazione, riavviare i pod netapp-ci-kube-state-metrics.
I pod netapp-ci-kube-state-metrics non riescono ad avviarsi dopo aver eseguito un aggiornamento dell'operatore Kubernetes, generando l'errore ErrImagePull (impossibilità di estrarre l'immagine).	Prova a reimpostare manualmente i pod.
Durante l'analisi dei log, vengono visualizzati i messaggi "Evento scartato perché più vecchio di maxEventAgeSeconds" per il mio cluster Kubernetes.	Modificare l'operatore *agentconfiguration* e aumentare *event-exporter-maxEventAgeSeconds* (ad esempio a 60 s), *event-exporter-kubeQPS* (ad esempio a 100) e *event-exporter-kubeBurst* (ad esempio a 500). Per maggiori dettagli su queste opzioni di configurazione, vedere"opzioni di configurazione" pagina.

Problema:	Prova questo:
Telegraf avvisa o si blocca a causa di una memoria bloccabile insufficiente.	Prova ad aumentare il limite di memoria bloccabile per Telegraf nel sistema operativo/nodo sottostante. Se aumentare il limite non è un'opzione, modificare la configurazione dell'agente NKMO e impostare *unprotected* su *true*. Ciò indicherà a Telegraf di non tentare di riservare pagine di memoria bloccate. Sebbene ciò possa rappresentare un rischio per la sicurezza, in quanto i segreti decrittati potrebbero essere trasferiti su disco, consente l'esecuzione in ambienti in cui non è possibile riservare memoria bloccata. Per maggiori dettagli sulle opzioni di configurazione *non protette*, fare riferimento a"opzioni di configurazione" pagina.
Vedo messaggi di avviso da Telegraf simili ai seguenti: *W! [inputs.diskio] Impossibile raccogliere il nome del disco per "vdc": errore durante la lettura di /dev/vdc: nessun file o directory del genere*	Per il Kubernetes Monitoring Operator, questi messaggi di avviso sono benigni e possono essere ignorati senza problemi. In alternativa, modifica la sezione telegraf in AgentConfiguration e imposta *runDsPrivileged* su true. Per maggiori dettagli, consulta il "opzioni di configurazione dell'operatore".

Problema:	Prova questo:

Il mio pod fluent-bit non funziona con i seguenti errori: [2024/10/16 14:16:23] [errore] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Troppi file aperti [2024/10/16 14:16:23] [errore] inizializzazione input tail.0 non riuscita [2024/10/16 14:16:23] [errore] [motore] inizializzazione input non riuscita	Prova a modificare le impostazioni *fsnotify* nel tuo cluster:
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	Riavvia Fluent-bit.
	Nota: per rendere queste impostazioni persistenti tra i riavvii del nodo, è necessario inserire le seguenti righe in */etc/sysctl.conf*
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problema:	Prova questo:
I pod DS di Telegraf segnalano errori relativi al plugin di input Kubernetes che non riesce a effettuare richieste HTTP a causa dell’impossibilità di convalidare il certificato TLS. Ad esempio: E! [inputs.kubernetes] Errore nel plugin: errore durante la richiesta HTTP a"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Ottenere"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: impossibile verificare il certificato: x509: impossibile convalidare il certificato per <kubelet_IP> perché non contiene alcun IP SAN	Ciò si verifica se il kubelet utilizza certificati autofirmati e/o il certificato specificato non include <kubelet_IP> nell'elenco *Subject Alternative Name* dei certificati. Per risolvere questo problema, l'utente può modificare il"configurazione dell'agente" e impostare *telegraf:insecureK8sSkipVerify* su *true*. In questo modo il plugin di input Telegraf verrà configurato per saltare la verifica. In alternativa, l'utente può configurare il kubelet per"serverTLSBootstrap" , che attiverà una richiesta di certificato dall'API 'certificates.k8s.io'.
Ricevo il seguente errore nei pod Fluent-bit e il pod non può essere avviato: 026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	Assicurarsi che la directory host in cui risiede il file DB disponga dei permessi di lettura/scrittura appropriati. Più specificamente, la directory host dovrebbe concedere permessi di lettura/scrittura agli utenti non root. Il percorso predefinito del file DB è /var/log/ a meno che non venga sovrascritto dall'opzione fluent-bit-dbFile *agentconfiguration*. Se SELinux è abilitato, provare a impostare l'opzione fluent-bit-seLinuxOptionsType agentconfiguration su 'spc_t'

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Opzioni di configurazione dell'operatore di monitoraggio Kubernetes

IL "Operatore di monitoraggio Kubernetes" Offre ampie opzioni di personalizzazione tramite il file AgentConfiguration. È possibile configurare limiti di risorse, intervalli di raccolta, impostazioni proxy, tolleranze e impostazioni specifiche per ogni componente per ottimizzare il monitoraggio del proprio ambiente Kubernetes. Utilizzare queste opzioni per personalizzare telegraf, kube-state-metrics, la raccolta dei log, la mappatura dei carichi di lavoro, la gestione delle modifiche e altri componenti di monitoraggio.

File di configurazione dell'agente di esempio

Di seguito è riportato un esempio di file *AgentConfiguration*, con descrizioni per ciascuna opzione.

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
```

```
    installed-by: nkmo-netapp-monitoring

spec:
  ##
  ## One can modify the following settings to configure and customize the
operator.
  ## Optional settings are commented out with their default values for
reference.
  ## To update them, uncomment the line, change the value, and apply the
updated AgentConfiguration.
  ##
  agent:
    ##
    ## [REQUIRED FIELD]
    ## A uniquely identifiable user-friendly cluster name
    ## The cluster name must be unique across all clusters in your Data
Infrastructure Insights (DII) environment.
    ##
    clusterName: "my_cluster"

    ##
    ## Proxy settings
    ## If applicable, specify the proxy through which the operator should
communicate with DII.
    ## Refer to additional documentation here:
    ## https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
    ##
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:

    ##
    ## [REQUIRED FIELD]
    ## Repository from which the operator pulls the required images
    ## By default, the operator pulls from the DII repository. To use a
private repository, set this field to the
    ## applicable repository name. Refer to additional documentation here:
    ## https://docs.netapp.com/us-
```

```
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
    ##
    dockerRepo: 'docker.c01.cloudinsights.netapp.com'
    ##
    ## [REQUIRED FIELD]
    ## Name of the imagePullSecret required for dockerRepo
    ## When using a private repository, set this field to the applicable
secret name.
    ##
    dockerImagePullSecret: 'netapp-ci-docker'

    ##
    ## Automatic expiring API key rotation settings
    ## Allow the operator to automatically rotate its expiring API key,
generating a new API key and
    ## using it to replace the expiring one. The expiring API key itself
must support auto rotation.
    ##
    # tokenRotationEnabled: 'true'
    ##
    ## Threshold (number of days before expiration) at which the operator
should trigger rotation.
    ## The threshold must be less than the total duration of the API key.
    ##
    # tokenRotationThresholdDays: '30'

  push-button-upgrades:
    ##
    ## Allow the operator to be upgraded using the Data Infrastructure
Insights (DII) UI
    ##
    # enabled: 'true'

    ##
    ## Frequency at which the operator polls and checks for upgrade
requests from DII
    ##
    # polltimeSeconds: '60'

    ##
    ## Allow operator upgrade to proceed even if new images are not
present
    ##
    # ignoreImageNotPresent: 'false'
```

```
    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreImageSignatureFailure: 'false'

    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreYAMLSignatureFailure: 'false'

    ##
    ## Use dockerImagePullSecret to access the image repository and verify
the existence of the new images
    ##
    # imageValidationUseSecret: 'true'

    ##
    ## Time allowed for the old operator pod to shutdown before reporting
an upgrade failure to DII
    ##
    # upgradesShutdownTime: '240'

    ##
    ## Time allowed for the new operator pod to startup before reporting
an upgrade failure to DII
    ##
    # upgradesStartupTime: '600'

  telegraf:
    ##
    ## Frequency at which telegraf collects data
    ## The frequency should not exceed 60s.
    ##
    # collectionInterval: '60s'

    ##
    ## Maximum number of metrics per batch
    ## Telegraf sends metrics to outputs in batches. This controls the
size of those writes.
    ##
    # batchSize: '10000'
```

```
    ##
    ## Maximum number of unwritten metrics per output
    ## Telegraf caches metrics until they are successfully written by the
output. This controls how many metrics
    ## can be cached. Once the buffer is filled, the oldest metrics will
get dropped.
    ##
    # bufferLimit: '150000'

    ##
    ## Rounds collection interval to collectionInterval
    ## If collectionInterval is 60s, collection will occur on-the-minute
    ##
    # roundInterval: 'true'

    ##
    ## Jitter between plugins on collection
    ## Each input plugin sleeps a random amount of time within jitter
before collecting. This can be used to prevent
    ## multiple input plugins from querying the same resources at the same
time. The maximum collection interval would
    ## be collectionInterval + collectionJitter.
    ##
    # collectionJitter: '0s'

    ##
    ## Precision to which collected metrics are rounded
    ## When set to "0s", precision will be set by the units specified by
collectionInterval.
    ##
    # precision: '0s'

    ##
    ## Frequency at which telegraf flushes and writes data
    ## Frequency should not exceed collectionInterval.
    ##
    # flushInterval: '60s'

    ##
    ## Jitter between plugins on writes
    ## Each output plugin sleeps a random amount of time within jitter
before flushing. This can be used to prevent
    ## multiple output plugins from writing the same resources at the same
time, and causing large spikes. The maximum
    ## flush interval would be flushInterval + flushJitter.
    ##
```

```
    # flushJitter: '0s'

    ##
    ## Timeout for HTTP output plugins
    ## Time allowed for http output plugins to successfully writing before
failing.
    ##
    # outputTimeout: '5s'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-ds DaemonSet
    ##
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
    # dsMemRequest: '500Mi'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-rs ReplicaSet
    ##
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    ##
    ## telegraf runs through the processor plugins a second time after the
aggregators plugins, by default. Use this
    ## option to skip the second run.
    ##
    # skipProcessorsAfterAggregators: 'false'

    ##
    ## Additional tolerations for netapp-ci-telegraf-ds DaemonSet and
netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet and netapp-ci-
telegraf-ds DaemonSet to view the default tolerations.
    ## If additional tolerations are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # dsTolerations: ''
    # rsTolerations: ''
```

```
    ##
    ## Additional node selector terms for netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet to view the default
node selectors terms. If additional node
    ## selector terms are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # rsNodeSelectorTerms: ''

    ##
    ## telegraf uses lockable memory to protect secrets in memory. If
telegraf issues warnings about insufficient
    ## lockable memory, try increasing the limit of lockable memory on the
applicable nodes. If increasing this limit
    ## is not an option for the given environment, set unprotected to true
so telegraf does not attempt to use
    ## lockable memory.
    ##
    # unprotected: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf-mountstats-
poller container in privileged mode
    ## The telegraf-mountstats-poller container needs read-only access to
system files such as those in /proc/ (i.e. to
    ## monitor NFS IO metrics, etc.). Some environments impose restricts
that prevent the container from reading these
    ## system files. Unless those restrictions are lifted, users may need
to run this container in privileged mode.
    ##
    # runPrivileged: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf container in
privileged mode
    ## The telegraf container needs read-only access to system files such
as those in /dev/ (i.e. for the telegraf
    ## diskio input plugin to retrieve disk metrics). Some environments
impose restricts that prevent the container from
    ## accessing these system files. Unless those restrictions are lifted,
```

```
users may need to run this container in
    ## privileged mode.
    ##
    # runDsPrivileged: 'false'

    ##
    ## Allow the netapp-ci-telegraf-ds DaemonSet's telegraf-ds, telegraf-
init, and telegraf-mountstats-poller containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## /proc/1/mountstats, etc.). Allowing escalation privilege should
negate the need to run these containers in
    ## privileged mode.
    ##
    # allowDsPrivilegeEscalation: 'true'

    ##
    ## Allow the netapp-ci-telegraf-rs DaemonSet's telegraf-rs and
telegraf-rs-init containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## etcd credentials when applicable, etc.). Allowing escalation
privilege should negate the need to run these
    ## containers in privileged mode.
    ##
    # allowRsPrivilegeEscalation: 'true'

    ##
    ## Enable collection of block IO metrics (kubernetes.pod_to_storage)
    ##
    # dsBlockIOEnabled: 'true'

    ##
    ## Enable collection of NFS IO metrics (kubernetes.pod_to_storage)
    ##
    # dsNfsIOEnabled: 'true'

    ##
    ## Enable collection of system-specific objects/metrics for managed
k8s clusters
    ## This consists of k8s objects within the kube-system and cattle-
system namespaces for managed k8s clusters
    ## (i.e. EKS, AKS, GKE, managed Rancher, etc.).
    ##
    # managedK8sSystemMetricCollectionEnabled: 'false'
```

```
    ##
    ## Enable collection of pod ephemeral storage metrics
(kubernetes.pod_volume)
    ##
    # podVolumeMetricCollectionEnabled: 'false'

    ##
    ## Declare Rancher cluster is managed
    ## Rancher can be deployed in managed or on-premise environments. The
operator contains logic to try to determine
    ## which type of environment Rancher is running in (i.e. to factor
into managedK8sSystemMetricCollectionEnabled).
    ## If the operator logic misidentifies whether Rancher is running in a
managed environment or not, use this option
    ## to declare Rancher is managed.
    ##
    # isManagedRancher: 'false'

    ##
    ## Locations for the etcd certificate and key files
    ## The operator looks at well-known locations for the etcd certificate
and key files. If this cannot find these
    ## files, the applicable telegraf input plugin will fail. Use this
option to specify the complete filepath to these
    ## files on the nodes.
    ## Note that the well-known locations for these files are typically
root-protected. This is one of the reasons why
    ## the netapp-ci-telegraf-rs ReplicaSet's telegraf-rs-init container
needs to run with escalation privileges.
    ##
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

    ##
    ## Allow operator/telegraf communications with k8s without TLS
verification
    ## In some environments, TLS verification will not succeed (i.e.
certificates lack IP SANs). To skip the
    ## verification, use this option.
    ##
    # insecureK8sSkipVerify: 'false'

  kube-state-metrics:
    ##
    ## CPU/Mem limits and requests for netapp-ci-kube-state-metrics
StatefulSet
```

```
    ##
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    ##
    ## Comma-separated list of k8s resources for which to collect metrics
    ## Refer to the kube-state-metrics --resources CLI option
    ##
    # resources:
'cronjobs,daemonsets,deployments,horizontalpodautoscalers,ingresses,jobs,n
amespaces,nodes,persistentvolumeclaims,persistentvolumes,pods,replicasets,
resourcequotas,services,statefulsets'

    ##
    ## Comma-separated list of k8s metrics to collect
    ## Refer to the kube-state-metrics --metric-allowlist CLI option
    ##
    # metrics:
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_
daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daem
onset_status_desired_number_scheduled,kube_daemonset_status_number_availab
le,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_
ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_obser
ved_generation,kube_daemonset_status_updated_number_scheduled,kube_daemons
et_metadata_generation,kube_daemonset_labels,kube_deployment_status_replic
as,kube_deployment_status_replicas_available,kube_deployment_status_replic
as_unavailable,kube_deployment_status_replicas_updated,kube_deployment_sta
tus_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec
_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_d
eployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_g
eneration,kube_deployment_labels,kube_deployment_created,kube_job_created,
kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_s
tatus_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_co
mpletion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_
status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec
_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube
_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persisten
tvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_ac
cess_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_label
s,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persiste
ntvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_comp
letion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_
status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_co
ntainer_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_c
```

```
ontainer_status_running,kube_pod_container_state_started,kube_pod_containe
r_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_c
ontainer_status_last_terminated_reason,kube_pod_container_status_ready,kub
e_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod
_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_p
od_init_container_info,kube_pod_init_container_status_waiting,kube_pod_ini
t_container_status_waiting_reason,kube_pod_init_container_status_running,k
ube_pod_init_container_status_terminated,kube_pod_init_container_status_te
rminated_reason,kube_pod_init_container_status_last_terminated_reason,kube
_pod_init_container_status_ready,kube_pod_init_container_status_restarts_t
otal,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod
_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource_
requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube_
pod_container_resource_requests_storage_bytes,kube_pod_container_resource_
requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_co
res,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_res
ource_limits_storage_bytes,kube_pod_container_resource_limits_ephemeral_st
orage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource_
limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset_
status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests,kube_horizontal
podautoscaler_spec_max_replicas,kube_horizontalpodautoscaler_spec_min_repl
icas,kube_horizontalpodautoscaler_status_condition,kube_horizontalpodautos
caler_status_current_replicas,kube_horizontalpodautoscaler_status_desired_
replicas'

    ##
    ## Comma-separated list of k8s label keys that will be used to
determine which labels to export/collect
    ## Refer to the kube-state-metrics --metric-labels-allowlist CLI
```

```
option
    ##
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],horizontalpodautoscalers=[*],
ingresses=[*],jobs=[*],namespaces=[*],nodes=[*],persistentvolumeclaims=[*]
,persistentvolumes=[*],pods=[*],replicasets=[*],resourcequotas=[*],service
s=[*],statefulsets=[*]'

    ##
    ## Additional tolerations for netapp-ci-kube-state-metrics StatefulSet
    ## Inspect the netapp-ci-kube-state-metrics StatefulSet to view the
default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # tolerations: ''

    ##
    ## Additional node selector terms for netapp-ci-kube-state-metrics
StatefulSet
    ## Inspect the kube-state-metrics StatefulSet to view the default node
selectors terms. If additional node selector
    ## terms are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # nodeSelectorTerms: ''

    ##
    ## Number of kube-state-metrics shards
    ## For large clusters, kube-state-metrics may be overwhelmed with
collecting and exporting the amount of metrics
    ## generated. This can lead to collection timeouts for the netapp-ci-
telegraf-rs pod. If this is observed, use this
    ## option to increase the number of kube-state-metrics shards to
redistribute the workload.
    ##
    # shards: '2'
```

```
  logs:
    ##
    ## Allow the netapp-ci-fluent-bit-ds DaemonSet's fluent-bit container
to run with escalation privilege.
    ## This is needed to access/read root-protected files (event-exporter
pod log, fluent-bit DB file, etc.).
    ##
    # fluent-bit-allowPrivilegeEscalation: 'true'

    ##
    ## Read content from the head of the file, not the tail
    ##
    # readFromHead: "true"

    ##
    ## Network protocol for DNS (i.e. UDP, TCP, etc.)
    ##
    # dnsMode: "UDP"

    ##
    ## DNS resolver (i.e. LEGACY, ASYNC, etc.)
    ##
    # fluentBitDNSResolver: "LEGACY"

    ##
    ## Additional tolerations for netapp-ci-fluent-bit-ds DaemonSet
    ## Inspect the netapp-ci-fluent-bit-ds DaemonSet to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # fluent-bit-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-fluent-bit-ds DaemonSet
    ##
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
    # fluent-bit-memRequest: '100Mi'

    ##
```

```
    ## Top-level host path in which the kubernetes container logs reside,
including any symlinks from var/log/containers
    ## For example, if /var/log/containers/*.log is a symlink to
/kubernetes/log to
    ## /kubernetes/var/lib/docker/containers/*/*.log, fluent-bit-
containerLogPath should be set to '/kubernetes'.
    ##
    # fluent-bit-containerLogPath: '/var/lib/docker/containers'

    ## fluent-bit DB file path/location

    ##
    ## fluent-bit DB file path/location
    ## By default, fluent-bit is configured to use /var/log/netapp-
monitoring_flb_kube.db.  This path usually requires
    ## escalated privileges for read/write. Users who want to avoid
escalation privilege can use this option to specify
    ## a different DB file path/location. The custom path/location should
allow non-root users to read/write.
    ## Ideally, the path/location should be persistent.
    ##
    # fluent-bit-dbFile: '/var/log/netapp-monitoring_flb_kube.db'

    ##
    ## Additional tolerations for netapp-ci-event-exporter Deployment
    ## Inspect the netapp-ci-event-exporter Deployment to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # event-exporter-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-event-exporter Deployment
    ##
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'

    ##
    ## Max age for events to be processed and exported; older events are
discarded
```

```
    ##
    # event-exporter-maxEventAgeSeconds: '10'

    ##
    ## Client-side throttling
    ## Set event-exporter-kubeBurst to roughly match event rate
    ## Set event-exporter-kubeQPS to approximately 1/5 of event-exporter-
kubeBurst
    ##
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    ##
    ## Additional node selector terms for netapp-ci-event-exporter
Deployment
    ## Inspect the event-exporter Deployment to view the default node
selectors terms. If additional node selector terms
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # event-exporter-nodeSelectorTerms: ''

  workload-map:
    ## Run workload-map container with escalation privilege to coordinate
memlocks
    ##
    ## Allow the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container to run with escalation privilege.
    ## This is needed to coordinate memlocks.
    ##
    # allowPrivilegeEscalation: 'true'

    ##
    ## CPU/Mem limits and requests for netapp-ci-net-observer-l4-ds
DaemonSet
    ##
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'
```

```
    ##
    ## Metric aggregation interval (in seconds)
    ## Set metricAggregationInterval between 30 and 120
    ##
    # metricAggregationInterval: '60'

    ##
    ## Interval for bpf polling
    ## Set bpfPollInterval between 3 and 15
    ##
    # bpfPollInterval: '8'

    ##
    ## Enable reverse DNS lookups on observed IPs
    ##
    # enableDNSLookup: 'true'

    ##
    ## Additional tolerations for netapp-ci-net-observer-l4-ds DaemonSet
    ## Inspect the netapp-ci-net-observer-l4-ds DaemonSet to view the
default tolerations. If additional tolerations
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # l4-tolerations: ''

    ##
    ## Run the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container in privileged mode
    ## Some environments impose restricts that prevent the net-observer
container from running.
    ## Unless those restrictions are lifted, users may need to run this
container in privileged mode.
    ##
    # runPrivileged: 'false'

  change-management:
    ##
    ## CPU/Mem limits and requests for netapp-ci-change-observer-watch-rs
ReplicaSet
    ##
    # cpuLimit: '1'
```

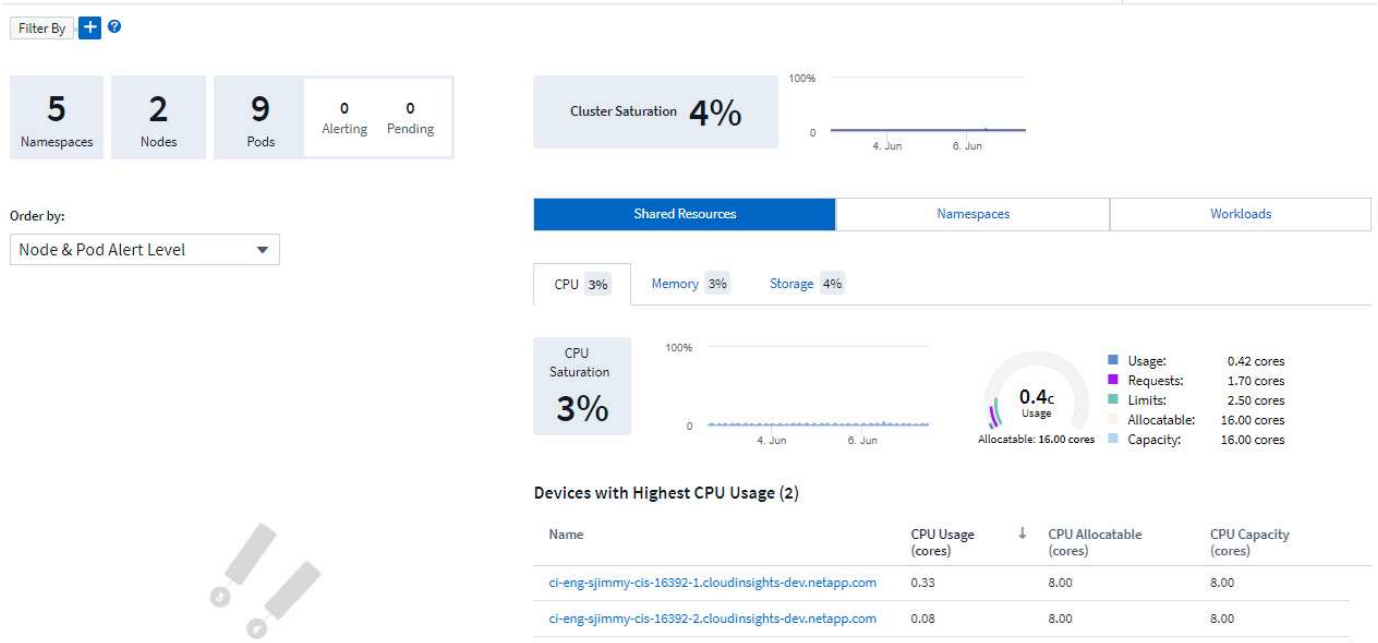
```
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    ##
    ## Interval (in seconds) after which a non-successful deployment of a
workload will be marked as failed
    ##
    # workloadFailureDeclarationIntervalSeconds: '30'

    ##
    ## Frequency (in seconds) at which workload deployments are combined
and sent
    ##
    # workloadDeployAggrIntervalSeconds: '300'

    ##
    ## Frequency (in seconds) at which non-workload deployments are
combined and sent
    ##
    # nonWorkloadDeployAggrIntervalSeconds: '15'

    ##
    ## Set of regular expressions used in env names and data maps whose
value will be redacted
    ##
    # termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

    ##
    ## Additional node selector terms for netapp-ci-change-observer-watch-
rs ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default node selectors terms. If additional
    ## node selector terms are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # nodeSelectorTerms: ''
```

```
    ##
    ## Comma-separated list of additional kinds to watch
    ## Each kind should be prefixed by its API group. This list in
addition to the default set of kinds watched by the
    ## collector.
    ##
    ## Example: '"authorization.k8s.io.subjectaccessreviews"'
    ##
    # additionalKindsToWatch: ''

    ##
    ## Comma-separated list of additional field paths whose diff is
ignored as part of change analytics
    ## This list in addition to the default set of field paths ignored by
the collector.
    ##
    ## Example: '"metadata.specTime", "data.status"'
    ##
    # additionalFieldsDiffToIgnore: ''

    ##
    ## Comma-separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    ## Each kind should be prefixed by its API group.
    ##
    ## Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
    ##
    # kindsToIgnoreFromWatch: ''

    ##
    ## Frequency with which log records are sent to DII from the collector
    ##
    # logRecordAggrIntervalSeconds: '20'

    ##
    ## Additional tolerations for netapp-ci-change-observer-watch-rs
ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
```

```
    # watch-tolerations: ''
```

Pagina dei dettagli del cluster Kubernetes

La pagina dei dettagli del cluster Kubernetes mostra una panoramica dettagliata del tuo cluster Kubernetes.



Conteggio di spazi dei nomi, nodi e pod

I conteggi nella parte superiore della pagina mostrano il numero totale di namespace, nodi e pod nel cluster, nonché il numero di popd attualmente in stato di avviso e in sospeso.

Risorse condivise e saturazione

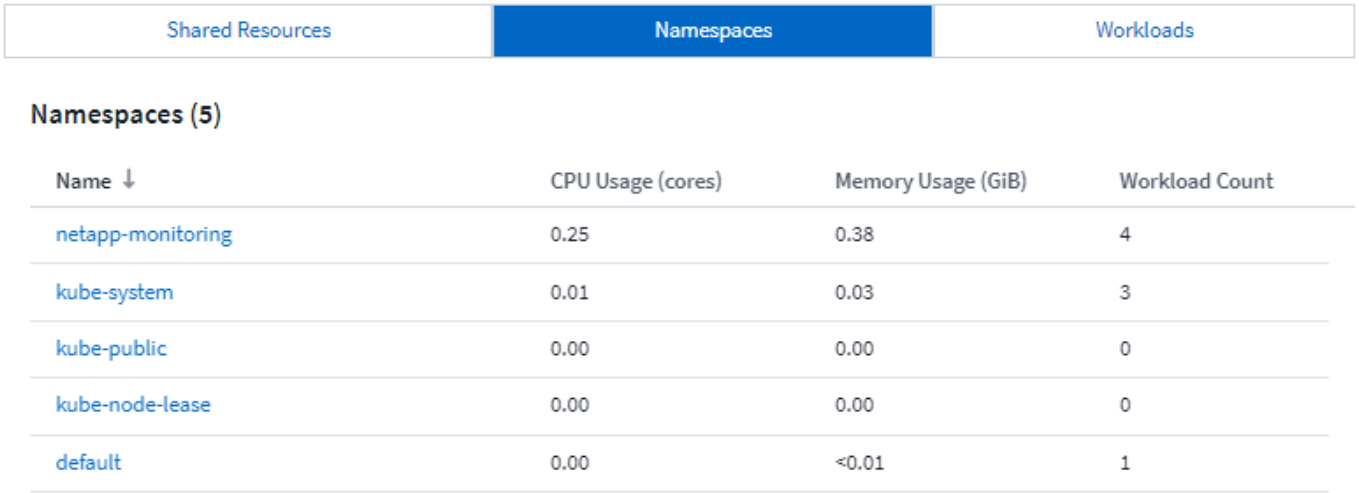
In alto a destra della pagina dei dettagli è visualizzata la saturazione del cluster in percentuale, nonché un grafico che mostra l'andamento recente nel tempo. La saturazione del cluster è il livello più alto di saturazione della CPU, della memoria o dello storage in ogni momento.

Al di sotto, la pagina mostra per impostazione predefinita l'utilizzo delle **Risorse condivise**, con schede per CPU, Memoria e Archiviazione. Ogni scheda mostra la percentuale di saturazione e l'andamento nel tempo, con ulteriori dettagli sull'utilizzo. Per l'archiviazione, il valore mostrato è il maggiore tra la saturazione del backend e quella del file system, calcolate in modo indipendente.

I dispositivi con il maggiore utilizzo sono mostrati in una tabella in basso. Clicca su un link qualsiasi per esplorare questi dispositivi.

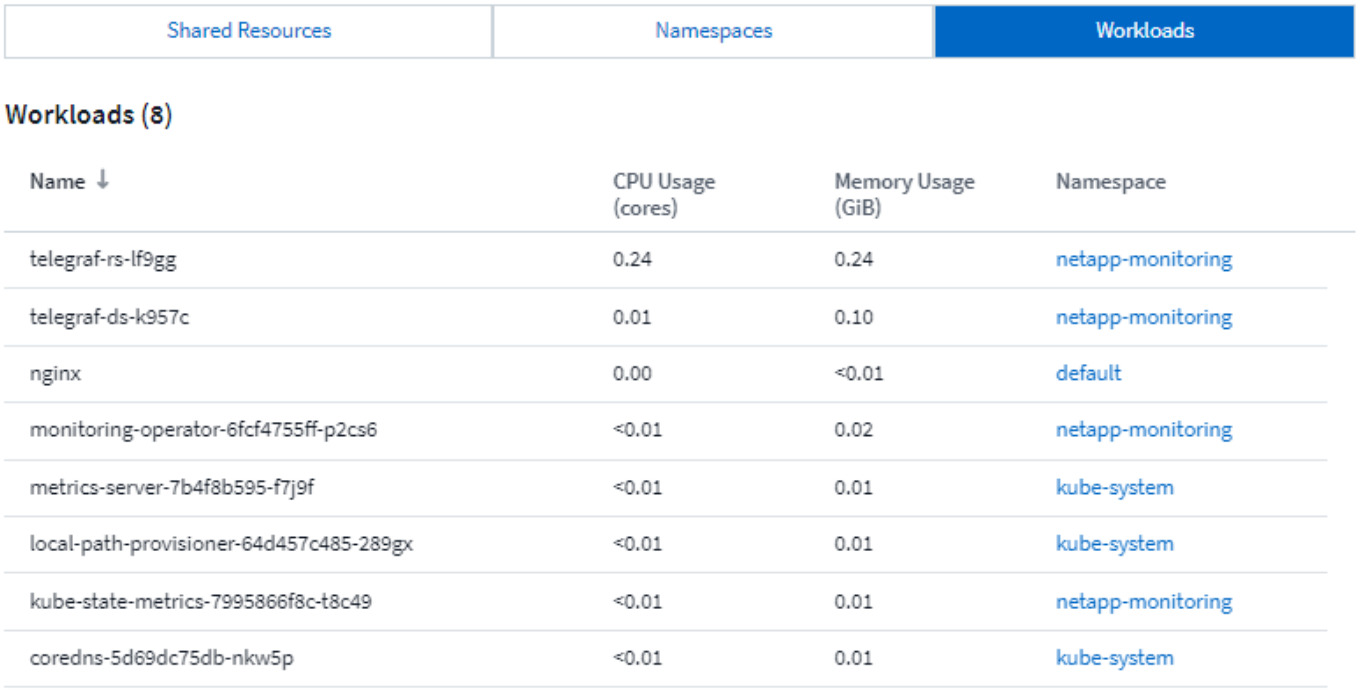
Spazi dei nomi

La scheda Namespace visualizza un elenco di tutti i namespace presenti nell'ambiente Kubernetes, mostrando l'utilizzo di CPU e memoria, nonché il conteggio dei carichi di lavoro in ciascun namespace. Fare clic sui collegamenti Nome per esplorare ogni spazio dei nomi.



Carichi di lavoro

Allo stesso modo, la scheda Carichi di lavoro visualizza un elenco dei carichi di lavoro in ogni namespace, mostrando ancora una volta l'utilizzo di CPU e memoria. Facendo clic sui collegamenti Namespace si accede a ciascuno di essi.



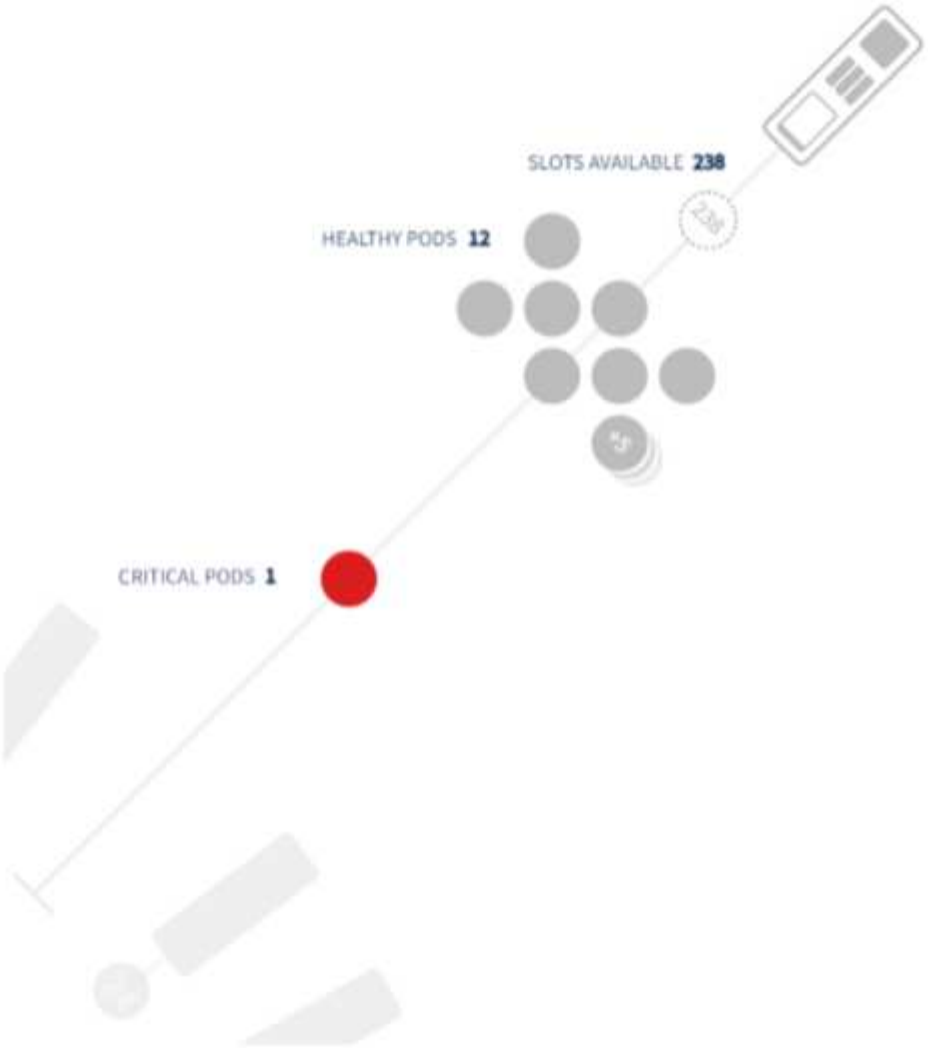
La "Ruota" del Cluster

La sezione "Ruota" del cluster fornisce una panoramica sullo stato di salute dei nodi e dei pod, su cui è possibile approfondire per ottenere maggiori informazioni. Se il cluster contiene più nodi di quanti ne possano essere visualizzati in quest'area della pagina, sarà possibile girare la rotellina utilizzando i pulsanti disponibili.

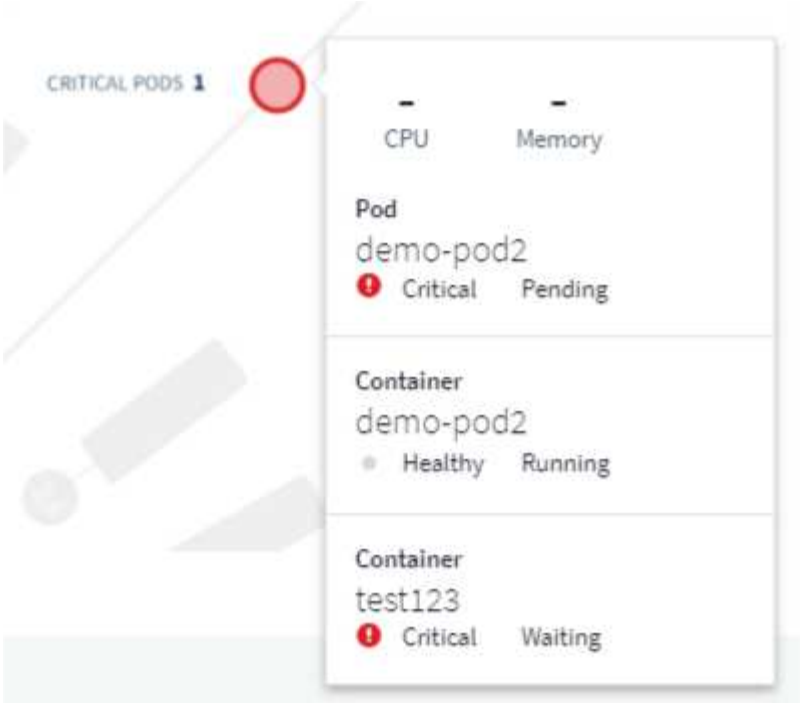
I pod o i nodi di avviso vengono visualizzati in rosso. Le aree di "Avvertenza" sono visualizzate in arancione. I pod non programmati (ovvero non collegati) verranno visualizzati nell'angolo inferiore della "Ruota" del cluster.

Passando il mouse sopra un pod (cerchio) o un nodo (barra) si estenderà la vista del nodo.

Facendo clic sul pod o sul nodo in quella vista, si ingrandirà la vista del nodo espansa.



Da qui puoi passare il mouse su un elemento per visualizzarne i dettagli. Ad esempio, passando il mouse sul pod critico in questo esempio vengono visualizzati i dettagli su quel pod.



È possibile visualizzare le informazioni su file system, memoria e CPU passando il mouse sugli elementi Node.

Una nota sugli indicatori

Gli indicatori di memoria e CPU mostrano tre colori, poiché mostrano la capacità *utilizzata* in relazione sia alla capacità *allocabile* che alla capacità *totale*.

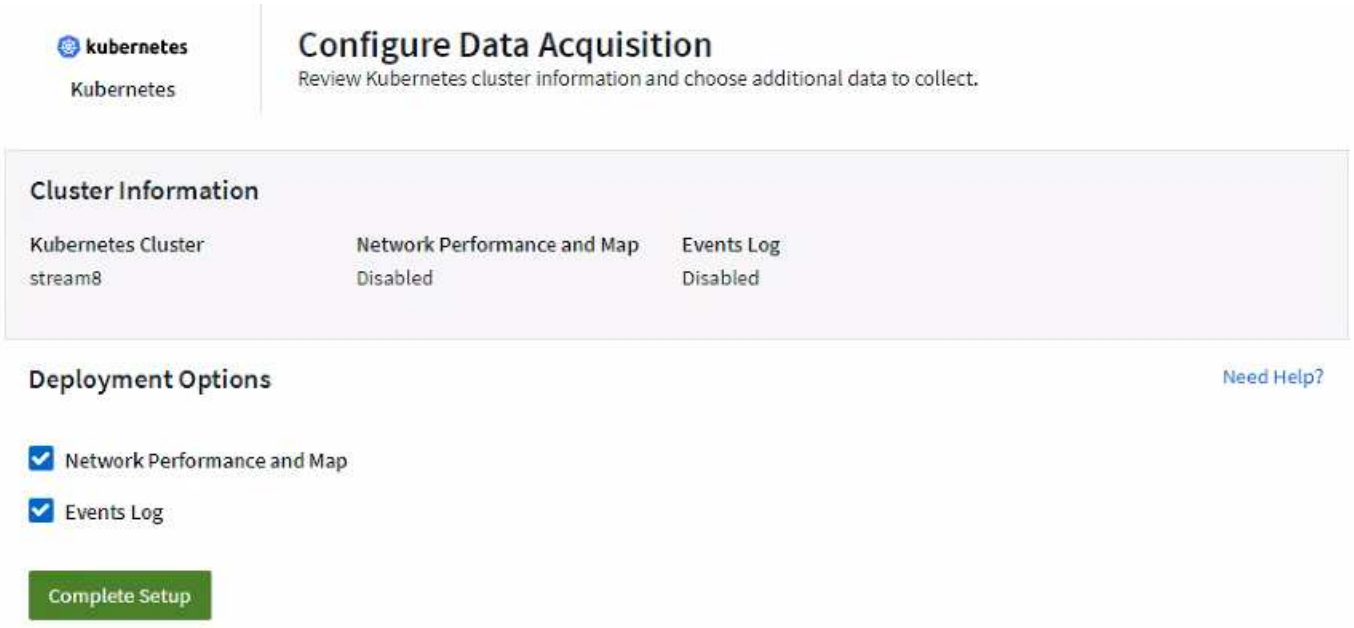
Monitoraggio e mappa delle prestazioni della rete Kubernetes

La funzionalità Kubernetes Network Performance Monitoring and Map semplifica la risoluzione dei problemi mappando le dipendenze tra i servizi (chiamati anche carichi di lavoro) e fornisce visibilità in tempo reale sulle latenze e sulle anomalie delle prestazioni di rete per identificare i problemi di prestazioni prima che influiscano sugli utenti. Questa funzionalità aiuta le organizzazioni a ridurre i costi complessivi analizzando e verificando i flussi di traffico di Kubernetes.

Caratteristiche principali: • La mappa del carico di lavoro presenta le dipendenze e i flussi del carico di lavoro di Kubernetes e mette in evidenza i problemi di rete e prestazioni. • Monitora il traffico di rete tra pod, carichi di lavoro e nodi Kubernetes; identifica l'origine del traffico e i problemi di latenza. • Ridurre i costi complessivi analizzando il traffico di rete in ingresso, in uscita, tra regioni e tra zone.

Prerequisiti

Prima di poter utilizzare Kubernetes Network Performance Monitoring and Map, è necessario aver configurato"Operatore di monitoraggio NetApp Kubernetes" per abilitare questa opzione. Durante l'implementazione dell'operatore, selezionare la casella di controllo "Prestazioni e mappa di rete" per abilitarla. Puoi anche abilitare questa opzione andando alla landing page di Kubernetes e selezionando "Modifica distribuzione".



Monitor

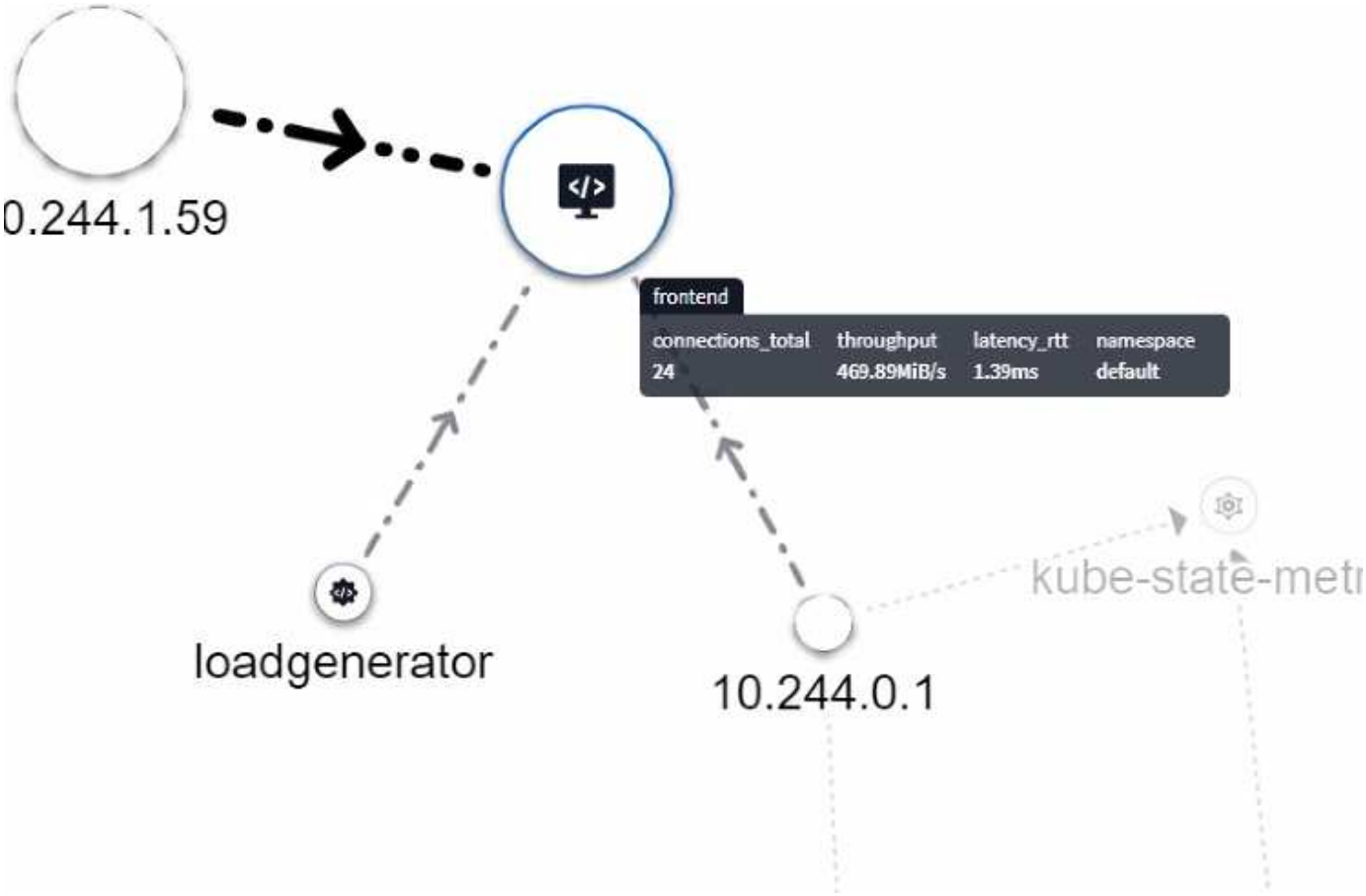
La mappa del carico di lavoro utilizza"monitor" per ricavare informazioni. Data Infrastructure Insights fornisce una serie di monitor Kubernetes predefiniti (si noti che questi potrebbero essere *in pausa* per impostazione predefinita). È possibile *Riprendere* (ovvero abilitare) i monitor desiderati oppure creare monitor personalizzati per gli oggetti Kubernetes, che verranno utilizzati anche da Workload Map.

È possibile creare avvisi sulle metriche di Data Infrastructure Insights su uno qualsiasi dei tipi di oggetti indicati di seguito. Assicurarsi che i dati siano raggruppati in base al tipo di oggetto predefinito.

- carico di lavoro di kubernetes
- kubernetes.daemonset
- distribuzione di kubernetes
- kubernetes.cronjob
- kubernetes.job
- kubernetes.replicaset
- kubernetes.statefulset
- kubernetes.pod
- kubernetes.network_traffic_l4

La mappa

La mappa mostra i servizi/carichi di lavoro e le loro relazioni reciproche. Le frecce indicano le direzioni del traffico. Passando il mouse sopra un carico di lavoro vengono visualizzate informazioni riepilogative per quel carico di lavoro, come puoi vedere in questo esempio:



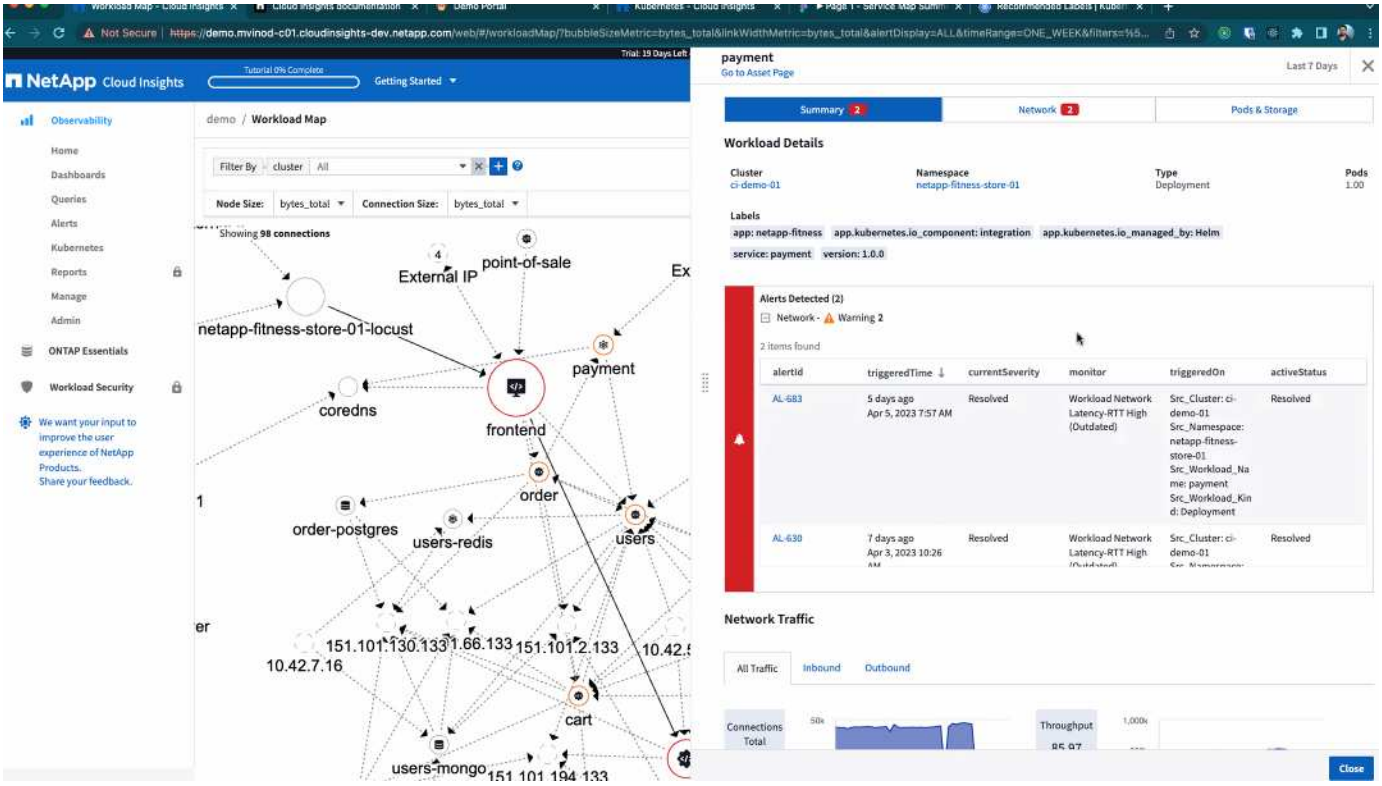
Le icone all'interno dei cerchi rappresentano diversi tipi di servizio. Si noti che le icone sono visibili solo se gli oggetti sottostanti hannoetichette .

La dimensione di ogni cerchio indica la dimensione del nodo. Tieni presente che queste dimensioni sono relative: il livello di zoom del tuo browser o le dimensioni dello schermo potrebbero influire sulle dimensioni effettive dei cerchi. Allo stesso modo, lo stile della linea di traffico fornisce una visione immediata delle dimensioni della connessione: le linee continue in grassetto indicano un traffico elevato, mentre le linee tratteggiate chiare indicano un traffico inferiore.

I numeri all'interno dei cerchi indicano il numero di connessioni esterne attualmente elaborate dal servizio.

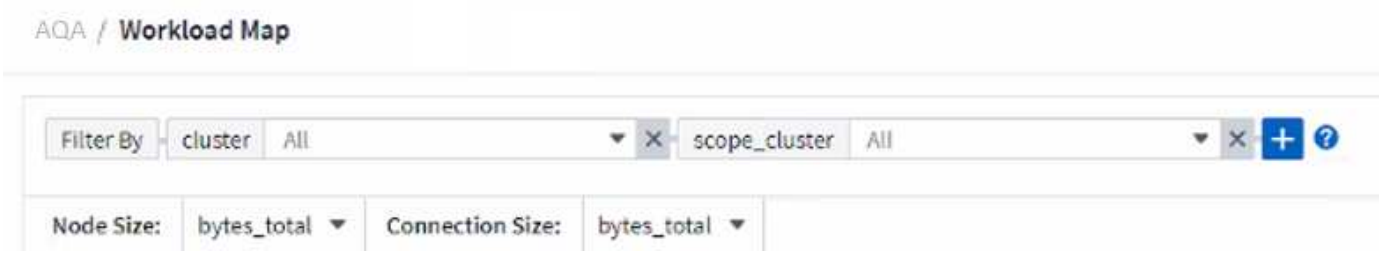
Dettagli e avvisi sul carico di lavoro

I cerchi colorati indicano un avviso di livello critico o di avvertimento per il carico di lavoro. Passa il mouse sul cerchio per un riepilogo del problema oppure clicca sul cerchio per aprire un pannello scorrevole con maggiori dettagli.

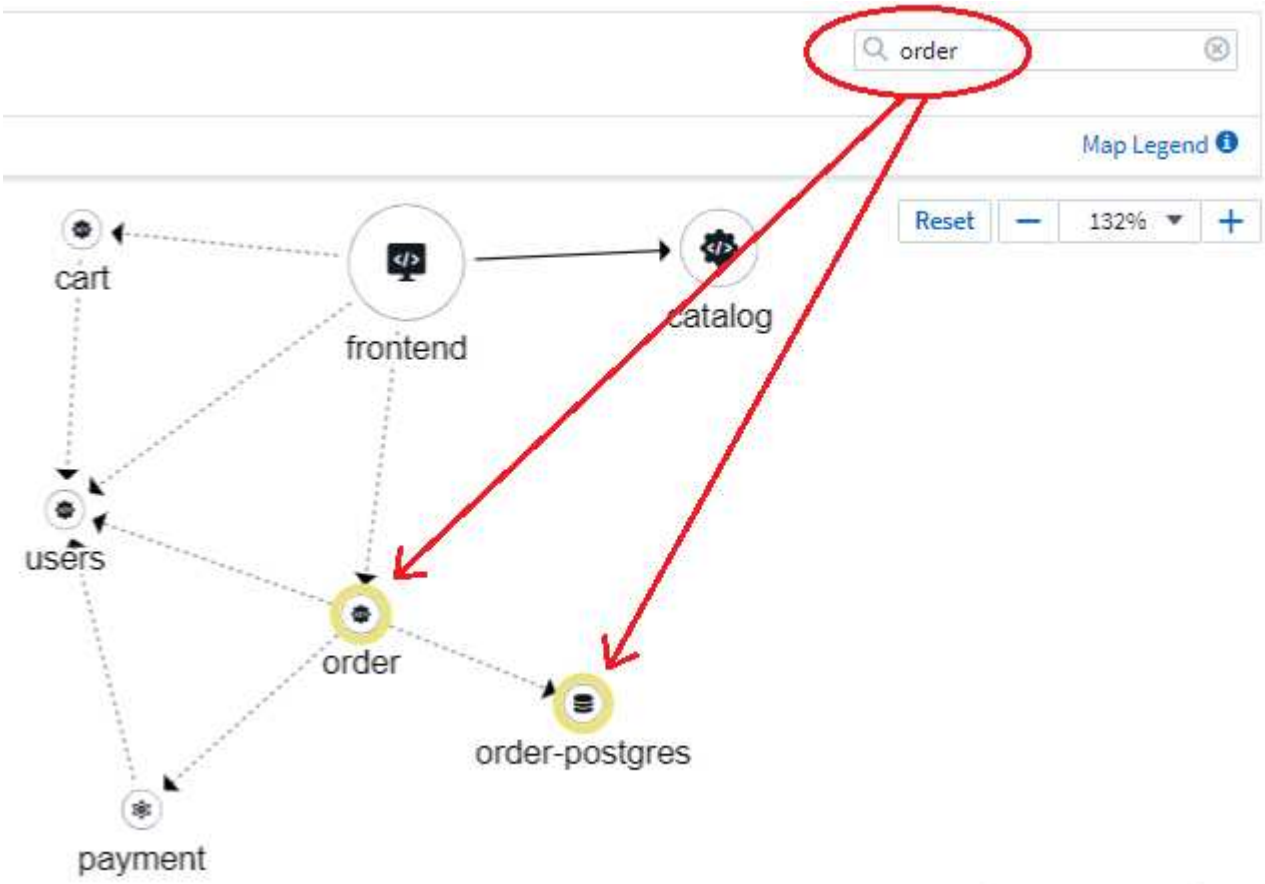


Ricerca e filtraggio

Come con altre funzionalità Data Infrastructure Insights , puoi facilmente impostare filtri per concentrarti sugli oggetti specifici o sugli attributi del carico di lavoro desiderati.



Allo stesso modo, digitando una stringa nel campo *Trova* verranno evidenziati i carichi di lavoro corrispondenti.



Etichette del carico di lavoro

Le etichette dei carichi di lavoro sono necessarie se si desidera che la mappa identifichi i tipi di carichi di lavoro visualizzati (ad esempio le icone circolari). Le etichette vengono derivate come segue:

- Nome del servizio/applicazione in esecuzione in termini generici
- Se la sorgente è un pod:
  - L'etichetta deriva dall'etichetta del carico di lavoro del pod
  - Etichetta prevista sul carico di lavoro: app.kubernetes.io/component
  - Riferimento nome etichetta: https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - Etichette consigliate:
    - fine frontale

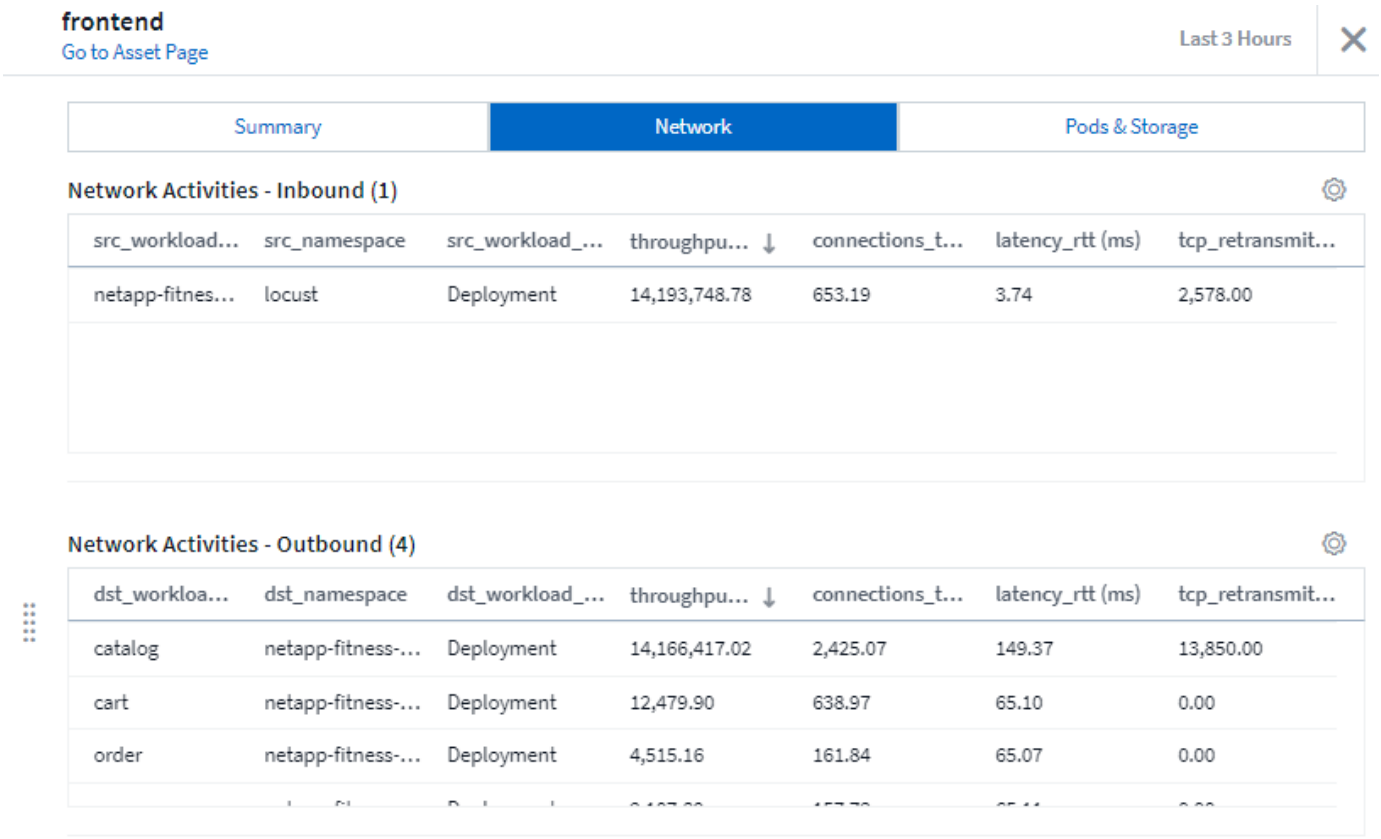
        - backend
        - banca dati
        - nascondiglio
        - coda
        - Kafka
- Se la sorgente è esterna al cluster Kubernetes:
    - Data Infrastructure Insights tenterà di analizzare il nome DNS risolto per estrarre il tipo di servizio.

      Ad esempio, con un nome DNS risolto di *s3.eu-north-1.amazonaws.com*, il nome risolto viene analizzato per ottenere *s3* come tipo di servizio.

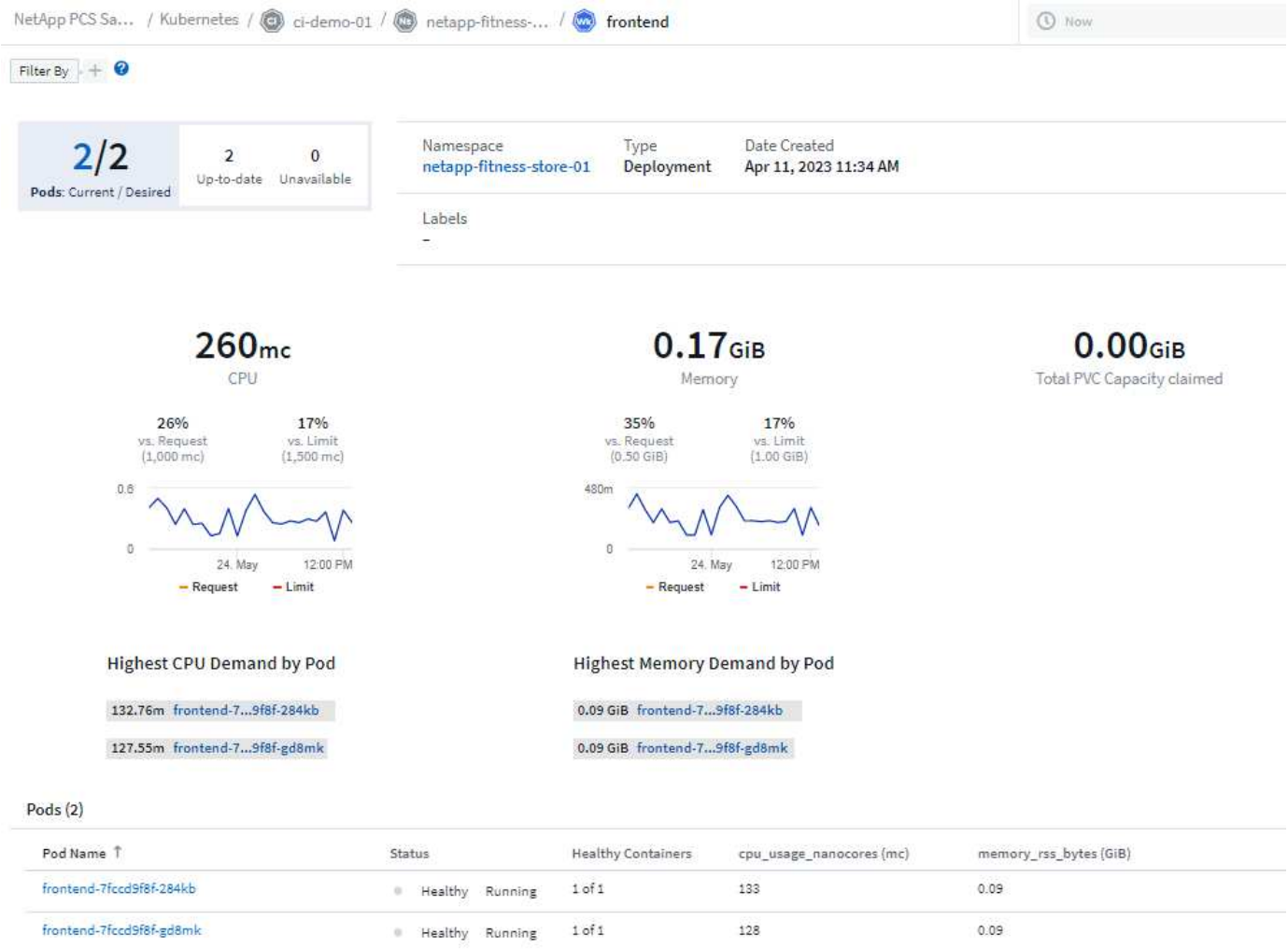
Immergiti in profondità

Facendo clic con il pulsante destro del mouse su un carico di lavoro vengono visualizzate opzioni aggiuntive da esplorare ulteriormente. Ad esempio, da qui è possibile ingrandire per visualizzare le connessioni per quel carico di lavoro.

In alternativa, è possibile aprire il pannello scorrevole dei dettagli per visualizzare direttamente la scheda *Riepilogo*, *Rete* o *Pod e archiviazione*.



Infine, selezionando *Vai alla pagina delle risorse* si aprirà la pagina di destinazione dettagliata delle risorse per il carico di lavoro.



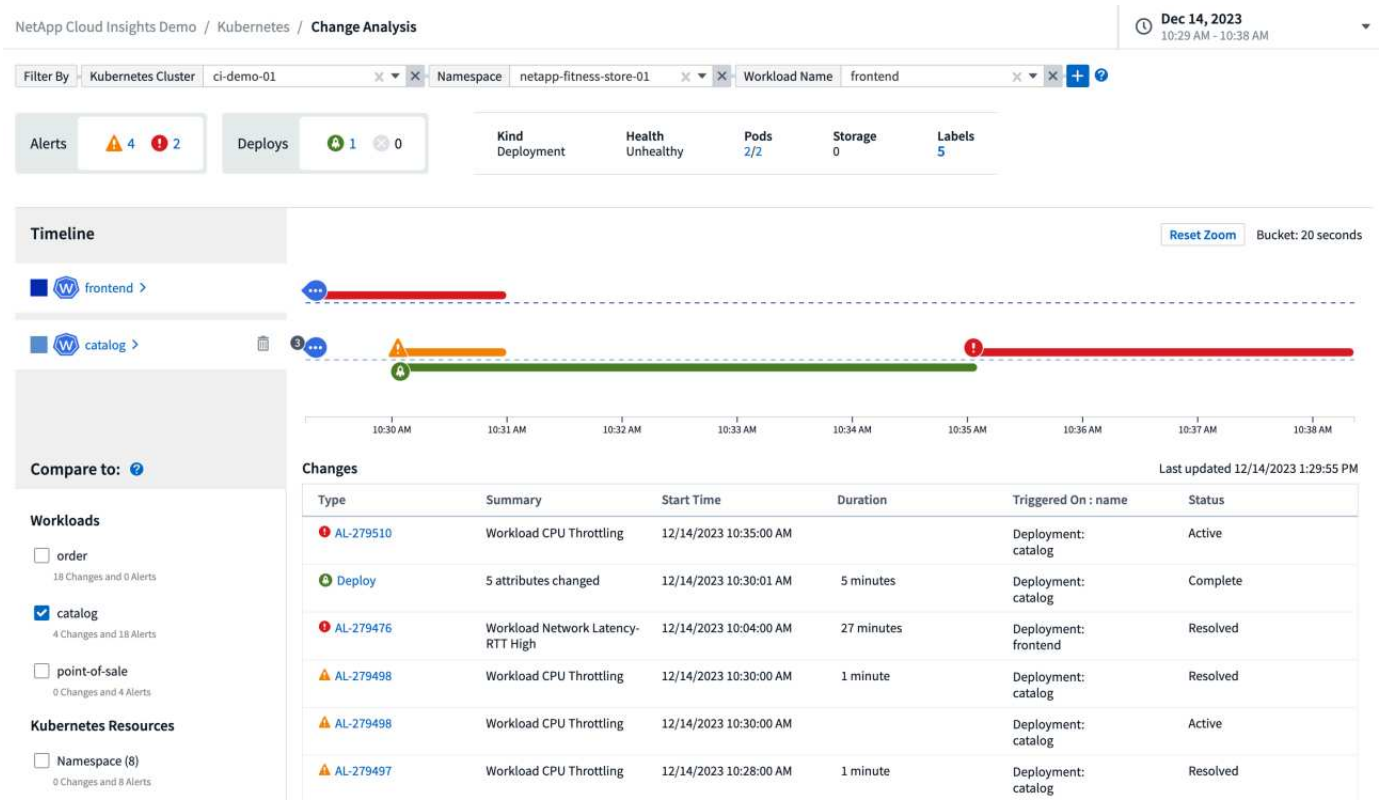
Analisi delle modifiche di Kubernetes

Kubernetes Change Analytics ti fornisce una visione completa delle modifiche recenti apportate al tuo ambiente K8s. Avvisi e stato di distribuzione sono a portata di mano. Con Change Analytics puoi monitorare ogni modifica di distribuzione e configurazione e correlarla allo stato di salute e alle prestazioni dei servizi, dell'infrastruttura e dei cluster di K8.

In che modo l'analisi del cambiamento può essere utile?

- Negli ambienti Kubernetes multi-tenant, le interruzioni possono verificarsi a causa di modifiche configurate in modo errato. Change Analytics aiuta in questo senso fornendo un unico riquadro per visualizzare e correlare lo stato dei carichi di lavoro e le modifiche alla configurazione. Ciò può aiutare nella risoluzione dei problemi degli ambienti Kubernetes dinamici.

Per visualizzare Kubernetes Change Analytics, vai su **Kubernetes > Change Analysis**.



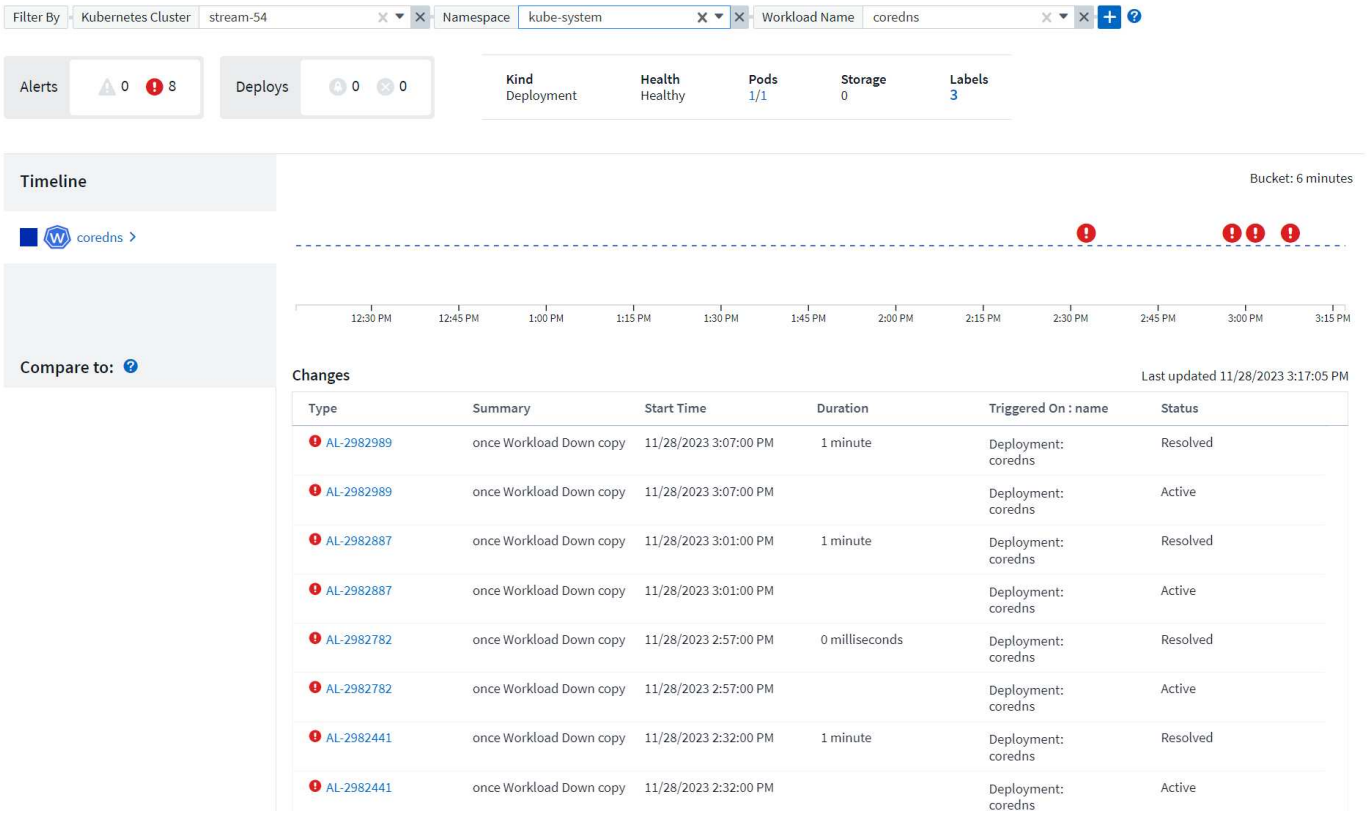
.

La pagina si aggiorna automaticamente in base all'intervallo di tempo Data Infrastructure Insights attualmente selezionato. Intervalli di tempo più brevi implicano aggiornamenti dello schermo più frequenti.

Filtraggio

Come per tutte le funzionalità di Data Infrastructure Insights, filtrare l'elenco delle modifiche è intuitivo: nella parte superiore della pagina, inserisci o seleziona i valori per il tuo cluster Kubernetes, namespace o workload, oppure aggiungi i tuoi filtri selezionando il pulsante {+].

Quando si filtra in base a un cluster, uno spazio dei nomi e un carico di lavoro specifici (insieme a tutti gli altri filtri impostati), viene visualizzata una cronologia delle distribuzioni e degli avvisi per quel carico di lavoro in quello spazio dei nomi su quel cluster. Per ingrandire ulteriormente la visualizzazione, fare clic e trascinare il grafico per concentrarsi su un intervallo di tempo più specifico.

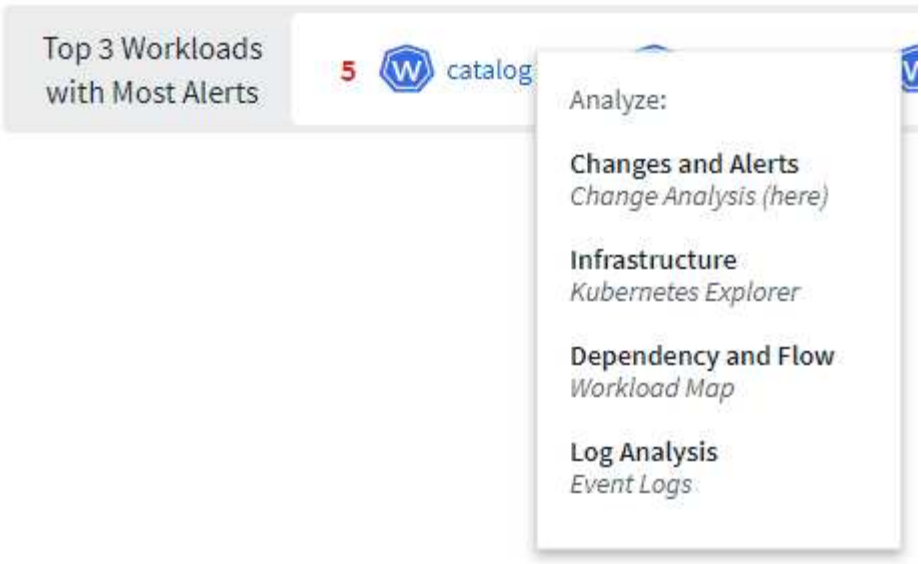


Stato rapido

Al di sotto dell'area di filtraggio si trovano una serie di indicatori di alto livello. Sulla sinistra è riportato il numero di avvisi (Avviso e Critico). Questo numero include sia gli avvisi *Attivi* che quelli *Risolti*. Per visualizzare solo gli avvisi *Attivi*, imposta un filtro per "Stato" e scegli "Attivo".

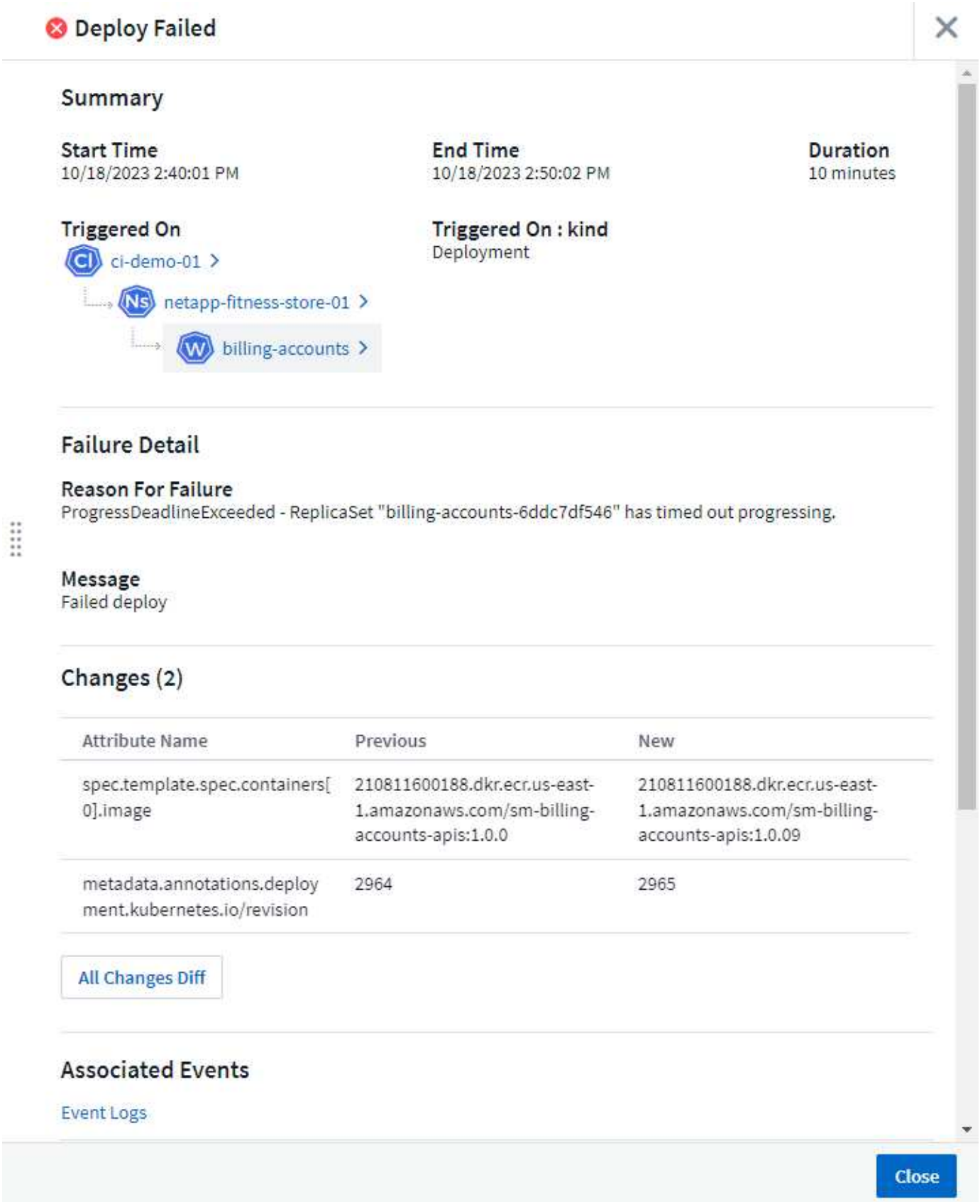
Qui viene mostrato anche lo stato di distribuzione. Anche in questo caso, l'impostazione predefinita è quella di mostrare il conteggio delle distribuzioni *Avviate*, *Completate* e *Non riuscite*. Per visualizzare solo le distribuzioni *Non riuscite*, imposta un filtro per "Stato" e seleziona "Non riuscito".

I successivi sono i 3 carichi di lavoro con il maggior numero di avvisi. Il numero in rosso accanto a ciascun carico di lavoro indica il numero di avvisi correlati a quel carico di lavoro. Fare clic sul collegamento del carico di lavoro per esplorare l'infrastruttura (Kubernetes Explorer), le dipendenze (mappa del carico di lavoro) o l'analisi dei registri (registri eventi).



Pannello di dettaglio

Selezionando una modifica nell'elenco si apre un pannello che descrive la modifica in modo più dettagliato. Ad esempio, selezionando una distribuzione non riuscita viene visualizzato un riepilogo della distribuzione, con orari di inizio e fine, durata e punto in cui è stata attivata la distribuzione, con collegamenti per esplorare tali risorse. Visualizza inoltre il motivo dell'errore, eventuali modifiche correlate ed eventuali eventi associati.



Anche selezionando un avviso si ottengono dettagli sull'avviso, tra cui il monitor che ha attivato l'avviso e un grafico che mostra una cronologia visiva dell'avviso.

Elementi essenziali ONTAP

ONTAP Essentials è un set di dashboard e flussi di lavoro che forniscono panoramiche dettagliate degli inventari e dei carichi di lavoro ONTAP . Quando si lavora in ONTAP Essentials, è possibile che vengano utilizzati i seguenti termini:

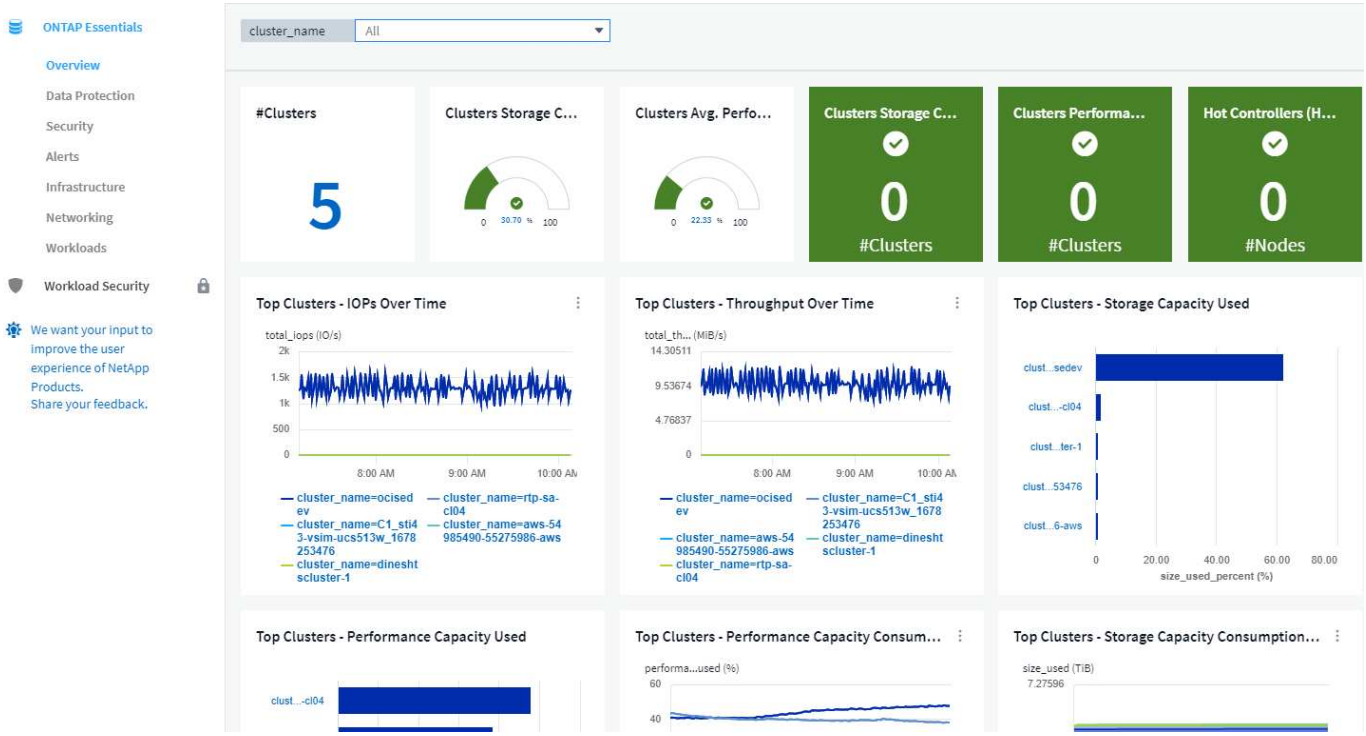
- Infrastruttura/inventario: oggetti che forniscono servizi di archiviazione/networking ai dati degli utenti
- Carichi di lavoro: oggetti che forniscono agli utenti un'interfaccia per leggere/scrivere dati.
- Protezione dei dati: oggetti che possono essere protetti utilizzando le tecnologie di protezione dei dati NetApp

Per ulteriori termini e definizioni relativi a ONTAP, vedere"Raccoglitore dati ONTAP" documentazione.

ONTAP Essentials richiede almeno un raccoglitore dati ONTAP funzionante con dati raccolti negli ultimi sette giorni.

Panoramica

Per iniziare l'esplorazione, seleziona * ONTAP Essentials* dal menu principale Data Infrastructure Insights .



La dashboard **Panoramica** mostra informazioni utili come il numero di cluster nel tenant con le relative percentuali di capacità e prestazioni complessive. Verranno inoltre visualizzati dati predittivi relativi al numero di giorni previsti prima che la capacità di archiviazione o la capacità di prestazione esauriscano lo spazio. Inoltre, se uno qualsiasi dei controller nella tua infrastruttura funziona con la CPU a più del 65%, mettendo potenzialmente a rischio il tuo cluster in caso di failover, ONTAP Essentials li mostra come controller "Hot".

I grafici informativi forniscono una panoramica delle prestazioni nel tempo e una ripartizione dell'utilizzo della capacità. Ciascuno di questi grafici o punti dati può essere utilizzato come punto di partenza per esplorazioni o indagini.

Nota: un numero pari a "0" (zero) indica che i giorni necessari per completare la prenotazione sono stimati in più di 90 giorni. In altre parole, i vostri sistemi non rischiano di esaurire lo spazio a breve.

Protezione dei dati

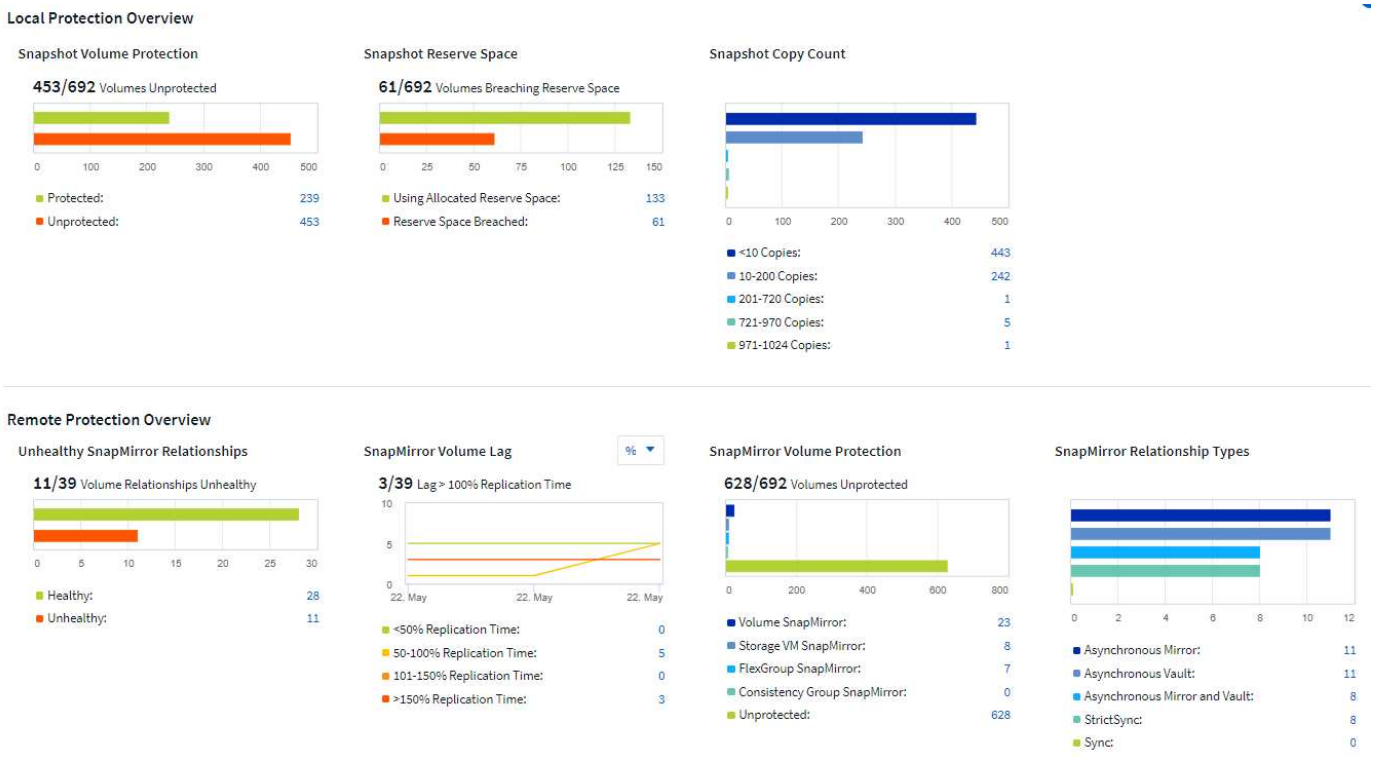
La pagina **Protezione dati** mostra lo stato dei volumi protetti da **copie snapshot** o *criteri SnapMirror *.

Nella sezione *Panoramica della protezione locale*, i grafici forniscono le seguenti informazioni per i volumi protetti da copie Snapshot:

- Numero di volumi protetti da copie Snapshot e di quelli non protetti.
- Numero di volumi che utilizzano o superano lo spazio di riserva per le copie Snapshot.
- Numero di volumi in intervalli specifici del conteggio delle copie Snapshot (ad esempio meno di 10 copie, da 10 a 200, ecc.).

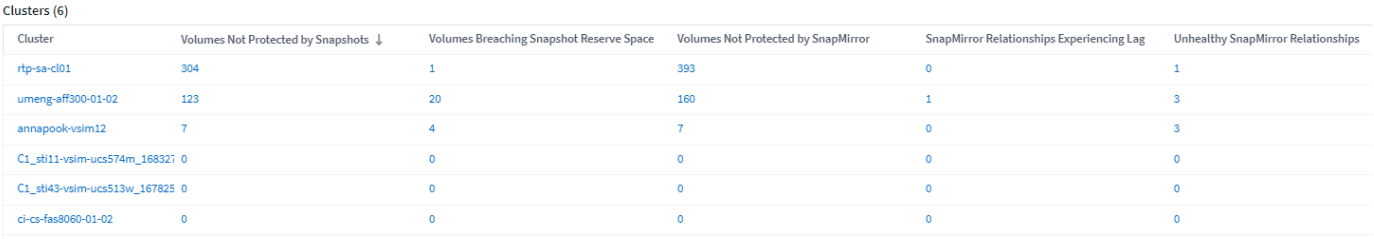
Nella sezione *Panoramica sulla protezione remota*, i grafici forniscono informazioni relative ai volumi protetti dai criteri SnapMirror :

- Il numero di relazioni SnapMirror sane e non sane.
- Numero di relazioni SnapMirror che presentano un ritardo nell'RPO (Recovery Point Objective) in base allo stato del ritardo.
- Numero di relazioni protette dai tipi di protezione del volume SnapMirror , quali Volume SnapMirror, relazioni SVMDR, relazioni FlexGroup SnapMirror , relazioni di gruppo di coerenza SnapMirror Business Continuity (SMBC), nonché volumi non protetti.
- Numero di relazioni protette dai tipi di relazione SnapMirror , quali Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync e Sync.



La griglia *Cluster* in fondo alla pagina fornisce dettagli relativi a quanto segue:

- Volumi non protetti da snapshot.
- Volumi che violano lo spazio di riserva degli snapshot.
- I volumi non protetti dalle policy di SnapMirror e le relazioni di SnapMirror presentano ritardi.
- Relazioni SnapMirror malsane.



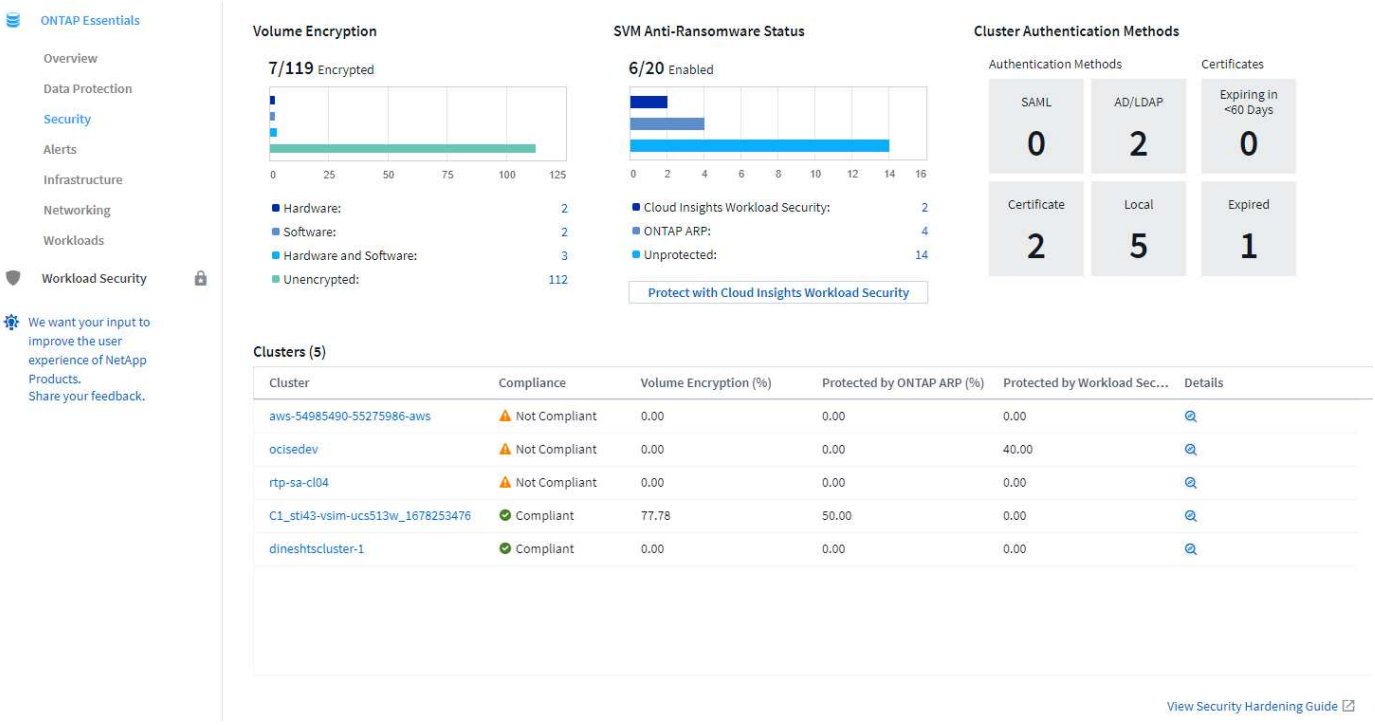
Clusters (6)

Cluster	Volumes Not Protected by Snapshots	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsim12	7	4	7	0	3
C1_sti11-vsim-ucs574m_168327	0	0	0	0	0
C1_sti43-vsim-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

Sicurezza

La Security Dashboard offre una panoramica immediata della situazione attuale della sicurezza, mostrando grafici relativi alla crittografia dei volumi hardware e software, allo stato di protezione contro la manomissione dei file e ai metodi di autenticazione dei cluster. I criteri di sicurezza vengono valutati in base alle raccomandazioni definite nel "* Guida al rafforzamento della sicurezza NetApp per ONTAP 9*".

Seleziona uno qualsiasi dei conteggi di crittografia o antimanomissione dei file per esplorare il tuo ambiente.

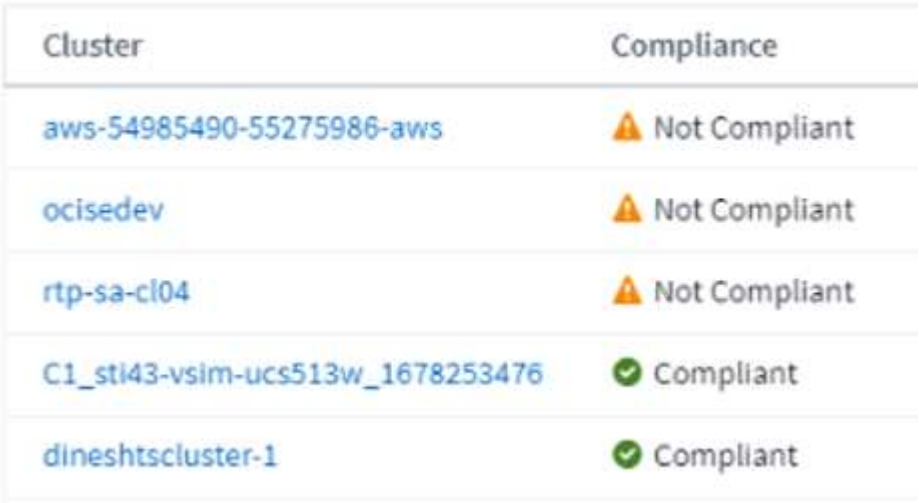


La dashboard di sicurezza ONTAP Essentials monitora l'ambiente per determinare lo stato di conformità del cluster. Fare riferimento al"Categorie di conformità del cluster" per saperne di più. ONTAP Essentials utilizza i seguenti monitor per determinare la conformità:

Nome del monitor	Nome attributo (visualizzato nei dettagli del cluster)	Valore conforme all'attributo
Modalità FIPS disabilitata	Modalità FIPS	Abilitato

Nome del monitor	Nome attributo (visualizzato nei dettagli del cluster)	Valore conforme all'attributo
Cifrari non sicuri del cluster per SSH	Impostazioni SSH sicure	SÌ
Protocollo Telnet abilitato	Telnet	Disabili
Shell remota abilitata	Shell remota	Disabili
Utente amministratore locale predefinito abilitato	Utente amministratore predefinito	Disabili
Password con hash MD5	MD5 in uso	NO
Comunicazione peer del cluster non crittografata	Cluster Peering	Crittografato/Nessun peer
AutoSupport HTTPS AutoSupport disabilitato	AutoSupport tramite HTTPS	SÌ
Nessun server NTP è configurato	Protocollo di tempo di rete	Configurato
Il numero di server NTP è basso	Protocollo di tempo di rete	Configurato
Banner di accesso al cluster disabilitato	Banner di accesso	Abilitato
Inoltro del registro non crittografato	Inoltro del registro crittografato	SÌ

Si noti che se un monitor sopra indicato è disabilitato, i dettagli del cluster mostreranno il valore "Non selezionato" per l'attributo di conformità alla sicurezza corrispondente.



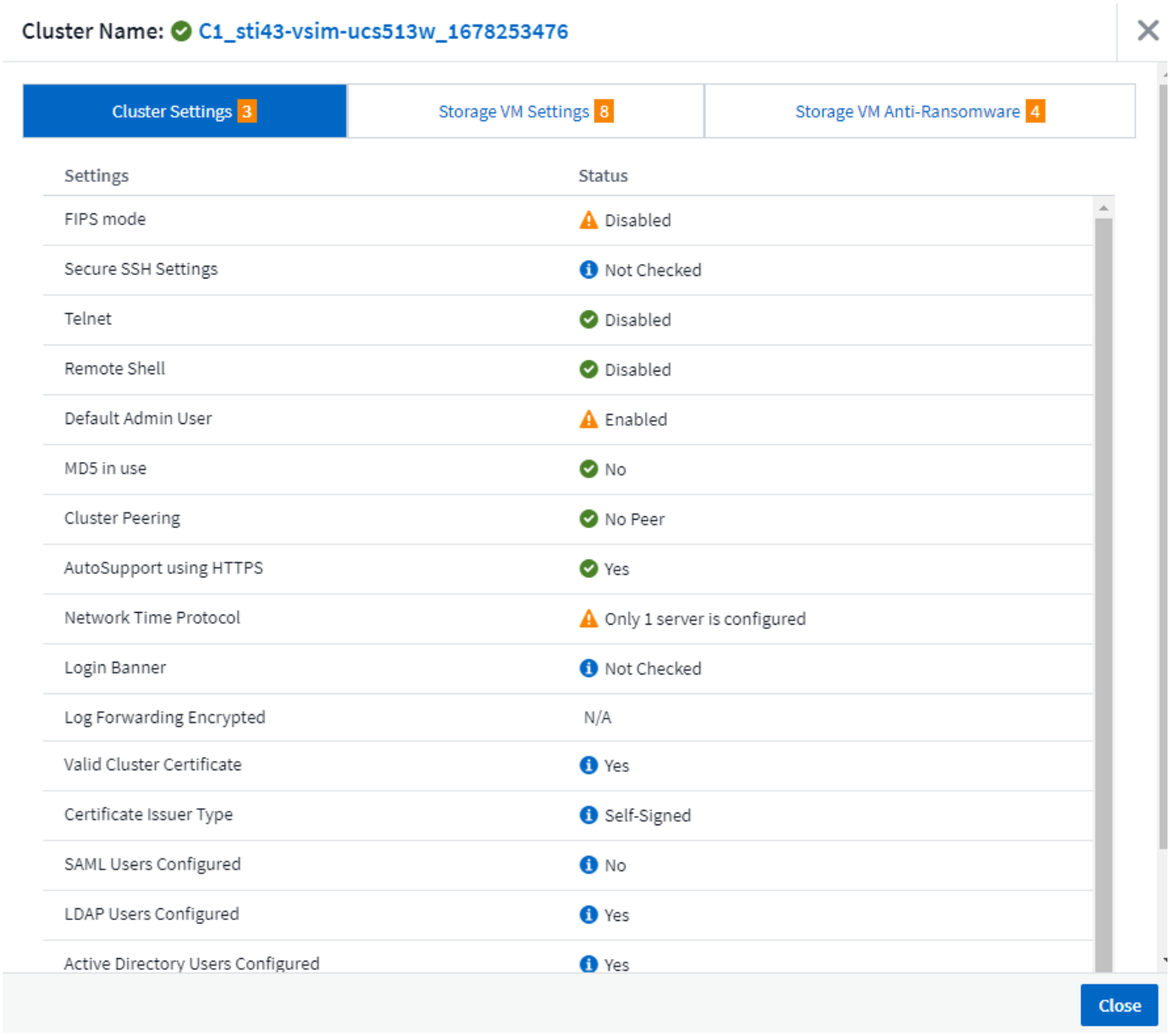
Per le SVM, la dashboard di sicurezza esamina i seguenti monitor:

Nome del monitor	Nome attributo (visualizzato nelle impostazioni della VM di archiviazione)	Valore conforme all'attributo
Cifrature non sicure per SSH nella VM di archiviazione	Impostazioni SSH sicure	SÌ

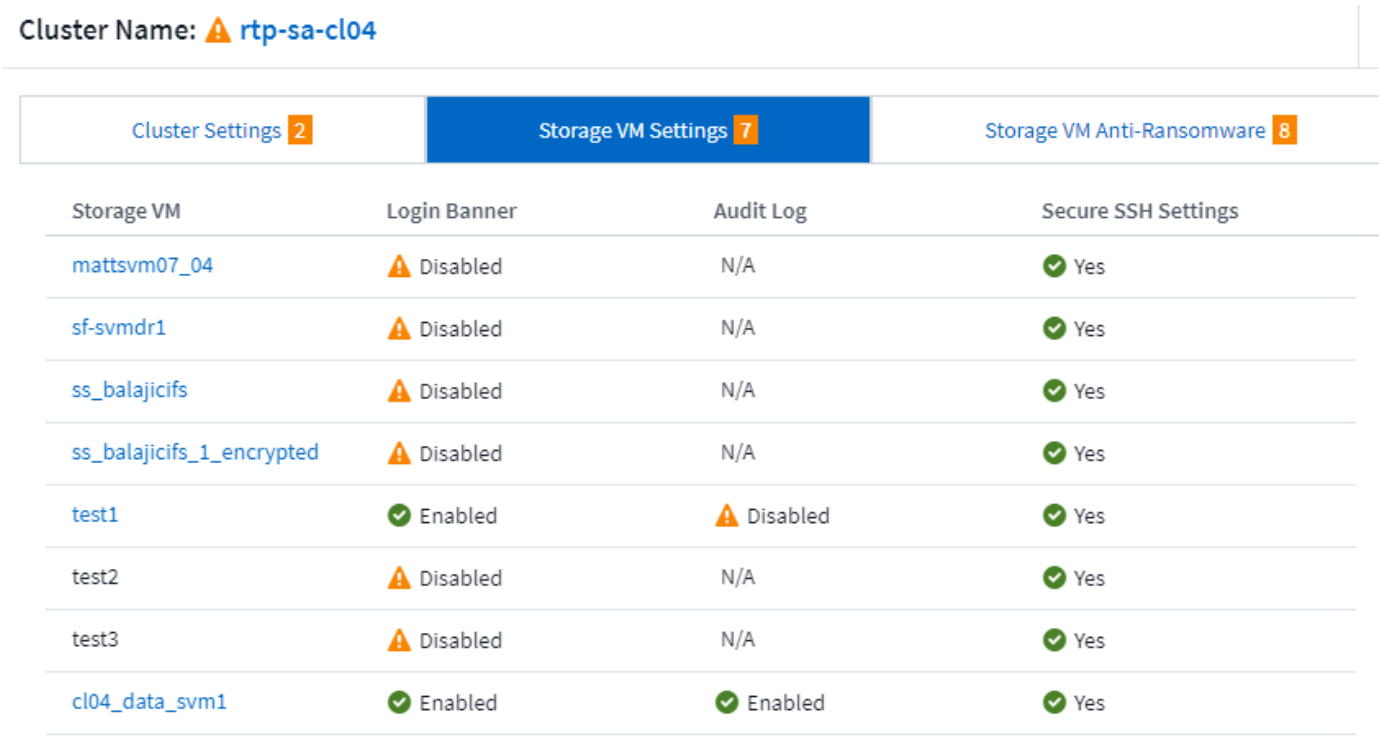
Nome del monitor	Nome attributo (visualizzato nelle impostazioni della VM di archiviazione)	Valore conforme all'attributo
Banner di accesso alla VM di archiviazione disabilitato	Banner di accesso	Abilitato
Registro di controllo della VM di archiviazione disabilitato	Registro di controllo	Abilitato

Nell'elenco dei cluster, seleziona *Visualizza dettagli* per ciascun cluster per aprire un pannello scorrevole che mostra le impostazioni correnti per *Cluster, Storage VM* o *Anti-Ransomware*.

I dettagli del cluster includono lo stato della connessione, le informazioni sul certificato e altro ancora:



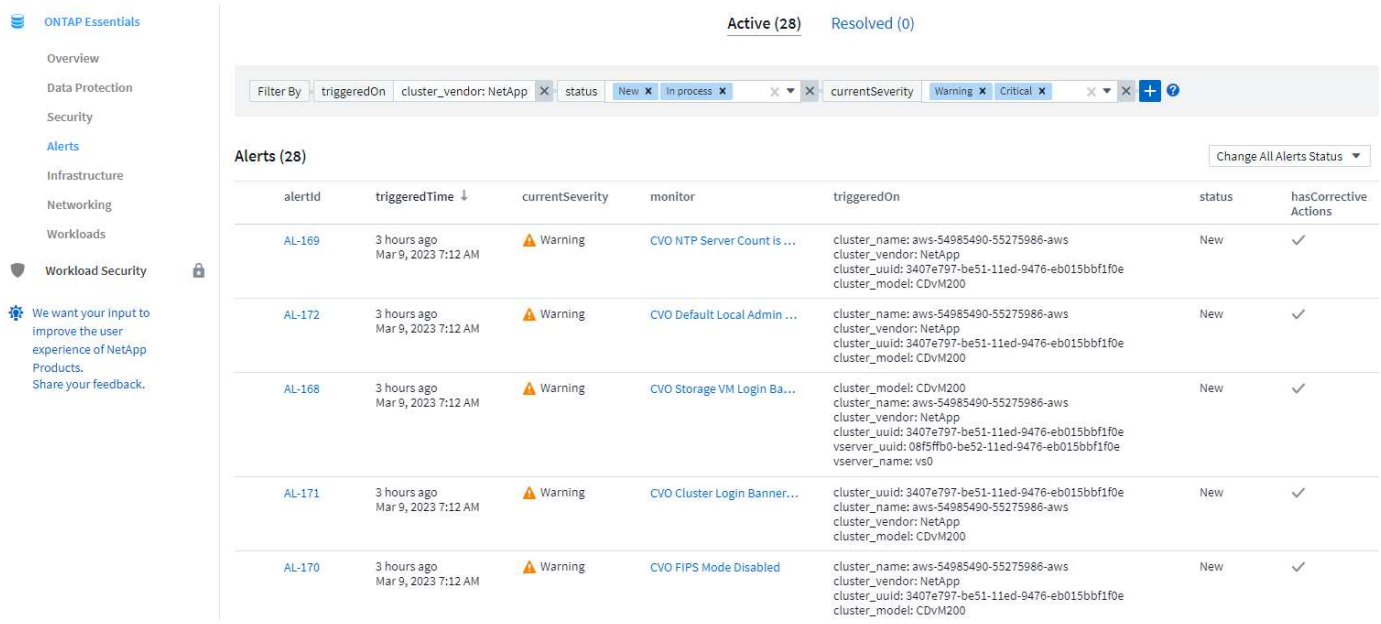
I dettagli della VM di archiviazione mostrano informazioni di audit e SSH:



I dettagli anti-ransomware mostrano se una VM di archiviazione è protetta dalla protezione anti-ransomware di ONTAP o dalla sicurezza del carico di lavoro Data Infrastructure Insights . Si noti che la colonna ONTAP ARP visualizza lo stato attuale della protezione anti-ransomware integrata di ONTAP, configurata sul sistema ONTAP . È possibile abilitare la sicurezza del carico di lavoro Data Infrastructure Insights selezionando "Proteggi" nella colonna
corrispondente.

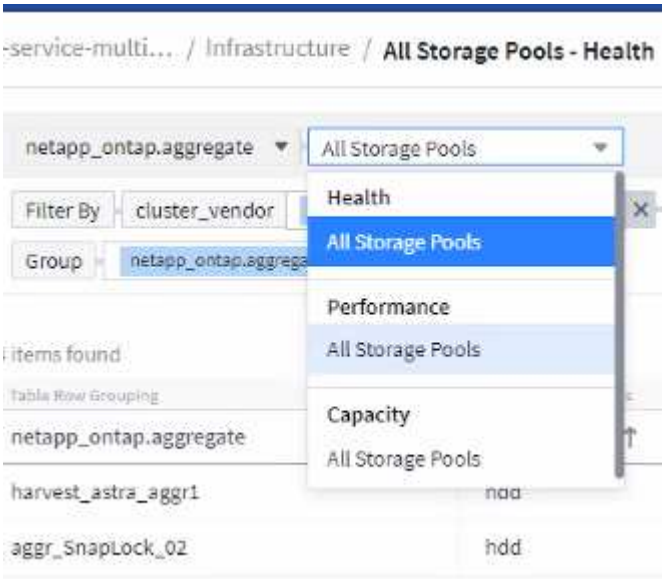
Avvisi

Qui puoi visualizzare gli avvisi attivi sul tuo tenant e analizzare rapidamente i potenziali problemi. Selezionare la scheda *Risolti* per visualizzare gli avvisi che sono stati risolti.

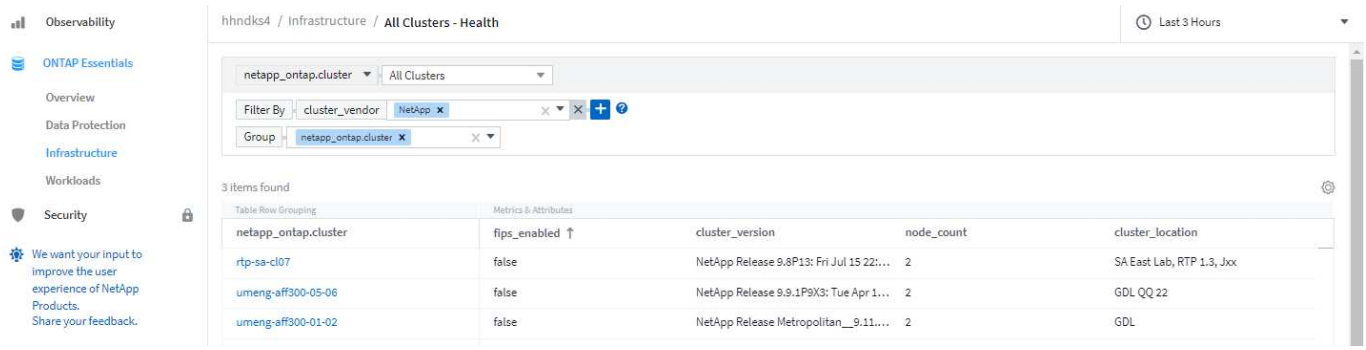


Infrastruttura

La pagina **Infrastruttura** ONTAP Essentials fornisce una panoramica dello stato di salute e delle prestazioni del cluster, utilizzando query predefinite (ma ulteriormente personalizzabili) su tutti gli oggetti ONTAP di base. Seleziona il tipo di oggetto che desideri esplorare (cluster, pool di archiviazione, ecc.) e scegli se visualizzare informazioni sullo stato o sulle prestazioni. Imposta i filtri per analizzare più a fondo i singoli sistemi.

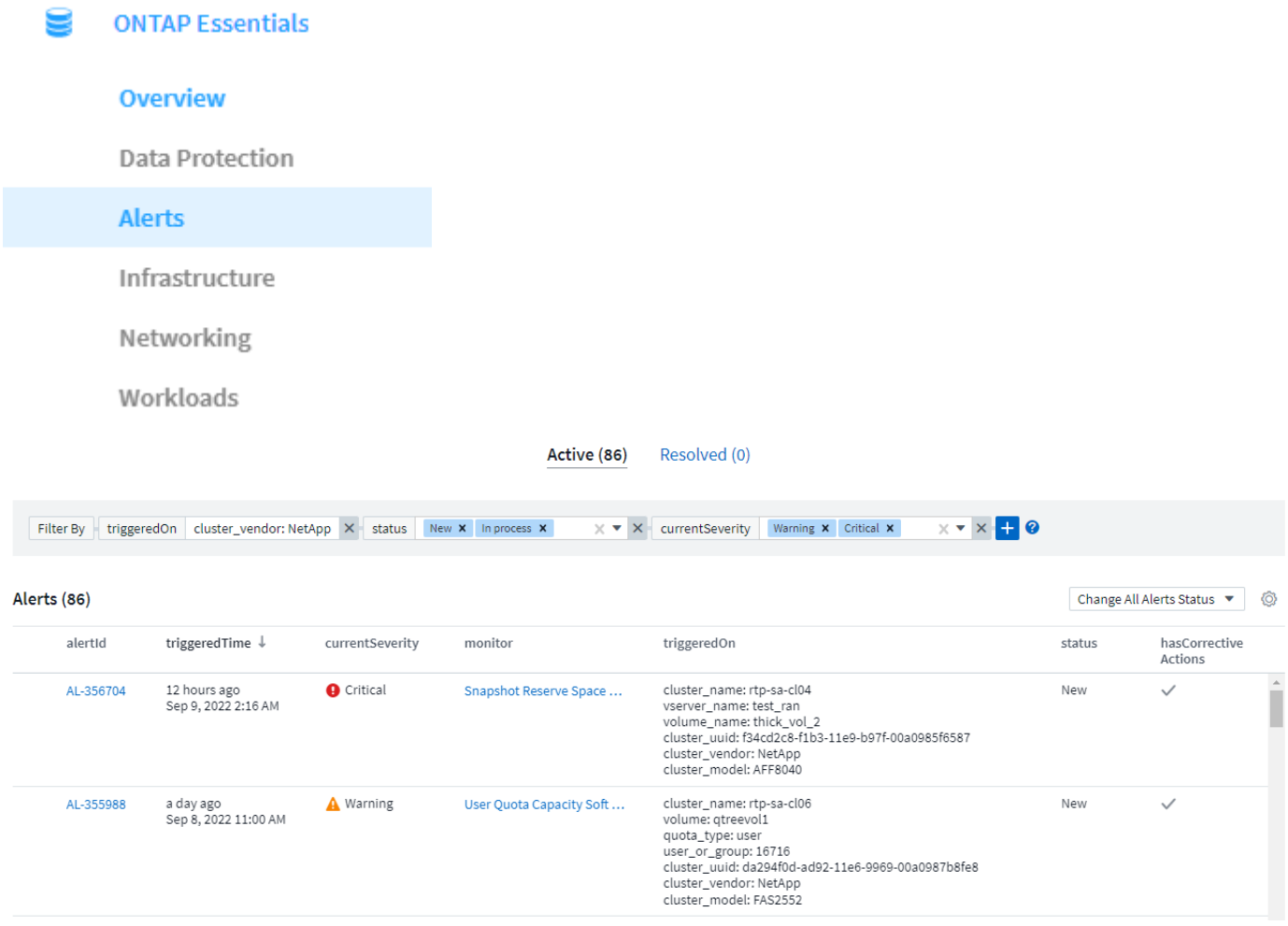


Pagina dell'infrastruttura che mostra lo stato di integrità del cluster:



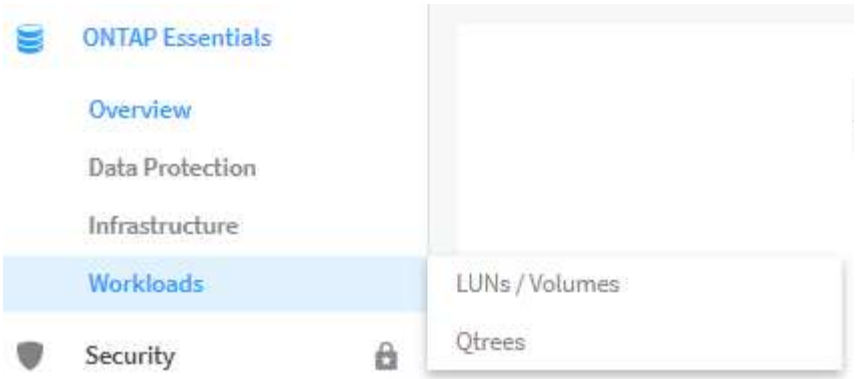
Networking

ONTAP Essentials Networking offre una panoramica della tua infrastruttura FC, NVME FC, Ethernet e iSCSI. In queste pagine puoi esplorare elementi quali le porte nei tuoi cluster e i loro nodi.



Carichi di lavoro

Visualizza ed esplora i carichi di lavoro su LUN/Volumi, condivisioni NFS o SMB o Qtree sul tuo tenant.



netapp_ontap.lun | All LUNs

Filter By | cluster_vendor | NetApp

Group | netapp_ontap.lun

13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late... ↑	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840....	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376....	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368....	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun_...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

Amministrazione e altre attività

API Data Infrastructure Insights

L'API Data Infrastructure Insights consente ai clienti NetApp e ai fornitori di software indipendenti (ISV) di integrare Data Infrastructure Insights con altre applicazioni, come CMDB o altri sistemi di ticketing.

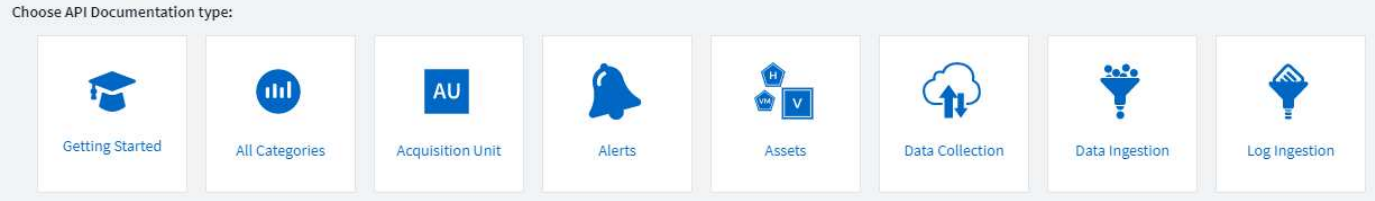
Le tue Data Infrastructure Insights"ruolo del set di funzionalità" determinerà a quali API potrai accedere. I ruoli Utente e Ospite hanno meno privilegi rispetto al ruolo Amministratore. Ad esempio, se hai il ruolo di Amministratore in Monitor e Ottimizza, ma il ruolo di Utente in Reporting, puoi gestire tutti i tipi di API tranne Data Warehouse.

Requisiti per l'accesso all'API

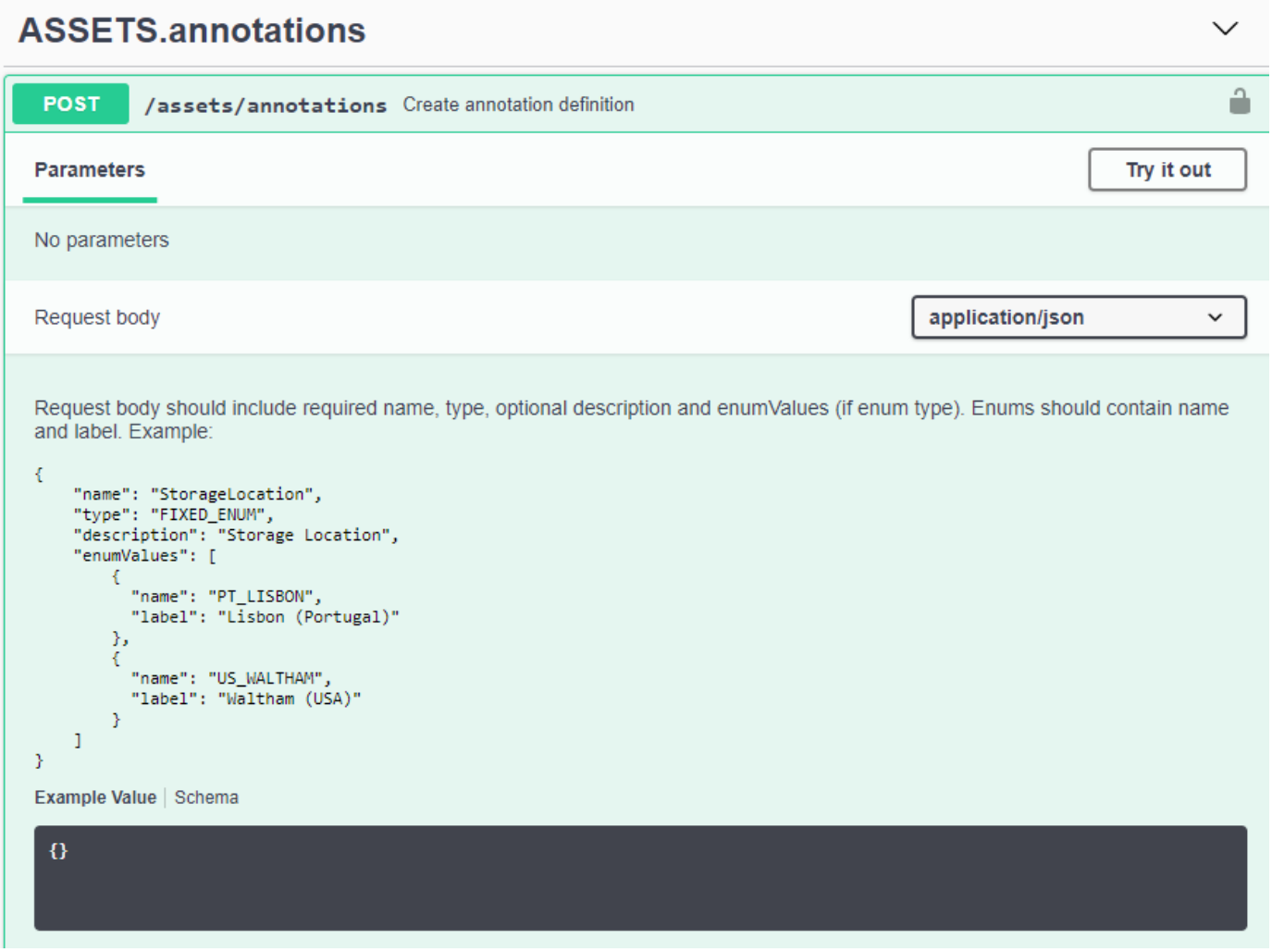
- Per concedere l'accesso viene utilizzato un modello di token di accesso API.
- La gestione dei token API viene eseguita dagli utenti Data Infrastructure Insights con il ruolo di amministratore.

Documentazione API (Swagger)

Le informazioni API più recenti sono reperibili accedendo a Data Infrastructure Insights e andando su **Amministrazione > Accesso API**. Fare clic sul collegamento **Documentazione API**.



La documentazione API è basata su Swagger, che fornisce una breve descrizione e informazioni sull'utilizzo dell'API e consente di provarla nel proprio tenant. A seconda del ruolo utente e/o dell'edizione Data Infrastructure Insights , i tipi di API disponibili potrebbero variare.



Token di accesso API

Prima di utilizzare l'API Data Infrastructure Insights , è necessario creare uno o più **token di accesso API**. I token di accesso vengono utilizzati per tipi di API specifici e possono concedere autorizzazioni di lettura e/o scrittura. È anche possibile impostare la scadenza per ciascun token di accesso. Tutte le API dei tipi specificati sono valide per il token di accesso. Ogni token è privo di nome utente o password.

Per creare un token di accesso:

- Fare clic su **Amministrazione > Accesso API**
- Fai clic su **+Token di accesso API**
  - Inserisci il nome del token
  - Seleziona i tipi di API
  - Specificare le autorizzazioni concesse per questo accesso API
  - Specificare la scadenza del token

> Il tuo token potrà essere copiato negli appunti e salvato solo durante il processo di creazione. Una volta creati, i token non possono essere recuperati, pertanto si consiglia vivamente di copiarli e salvarli in un luogo sicuro. Ti verrà chiesto di fare clic sul pulsante **Copia token di accesso API** prima di poter chiudere la schermata di creazione del token.

È possibile disattivare, attivare e revocare i token. I token disabilitati possono essere abilitati.

I token garantiscono l'accesso generico alle API dal punto di vista del cliente, gestendo l'accesso alle API nell'ambito del proprio tenant. Gli amministratori dei clienti possono concedere e revocare questi token senza il coinvolgimento diretto del personale back-end di Data Infrastructure Insights .

L'applicazione riceve un token di accesso dopo che un utente si è autenticato e ha autorizzato l'accesso, quindi passa il token di accesso come credenziale quando chiama l'API di destinazione. Il token trasmesso informa l'API che il portatore del token è stato autorizzato ad accedere all'API ed eseguire azioni specifiche specificate dall'ambito concesso durante l'autorizzazione.

L'intestazione HTTP in cui viene passato il token di accesso è **X-CloudInsights-ApiKey:**.

Ad esempio, utilizzare quanto segue per recuperare le risorse di archiviazione:

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
Dove _<API_Access_Token>_ è il token salvato durante la creazione
dell'accesso API.
```

Consulta le pagine Swagger per esempi specifici per l'API che desideri utilizzare.

Tipo di API

L'API Data Infrastructure Insights è basata su categorie e attualmente contiene i seguenti tipi:

- Il tipo ASSETS contiene API per asset, query e ricerca.
  - Risorse: enumera gli oggetti di livello superiore e recupera un oggetto specifico o una gerarchia di oggetti.
  - Query: recupera e gestisci le query di Data Infrastructure Insights .
  - Importa: importa annotazioni o applicazioni e assegnale agli oggetti
  - Cerca: individua un oggetto specifico senza conoscerne l'ID univoco o il nome completo.
- Il tipo RACCOLTA DATI viene utilizzato per recuperare e gestire i raccoglitori di dati.
- Il tipo DATA INGESTION viene utilizzato per recuperare e gestire i dati di ingestione e le metriche personalizzate, ad esempio dagli agenti Telegraf
- LOG INGESTION viene utilizzato per recuperare e gestire i dati di registro

Nel tempo potrebbero diventare disponibili altri tipi e/o API. Puoi trovare le informazioni API più recenti in"Documentazione API Swagger" .

Si noti che i tipi di API a cui un utente ha accesso dipendono anche da"Ruolo utente" dispongono in ogni set di funzionalità Data Infrastructure Insights (monitoraggio, sicurezza del carico di lavoro, reporting).

Attraversamento dell'inventario

Questa sezione descrive come attraversare una gerarchia di oggetti Data Infrastructure Insights .

Oggetti di primo livello

I singoli oggetti vengono identificati nelle richieste tramite un URL univoco (chiamato "self" in JSON) e richiedono la conoscenza del tipo di oggetto e dell'ID interno. Per alcuni degli oggetti di livello superiore (host, storage e così via), l'API REST fornisce l'accesso alla raccolta completa.

Il formato generale di un URL API è:

```
 https://<tenant>/rest/v1/<type>/<object>
Ad esempio, per recuperare tutti gli archivi da un tenant denominato
_mysite.c01.cloudinsights.netapp.com_, l'URL della richiesta è:
```

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Bambini e oggetti correlati

Gli oggetti di livello superiore, come Storage, possono essere utilizzati per passare ad altri oggetti figlio e correlati. Ad esempio, per recuperare tutti i dischi per uno storage specifico, concatenare l'URL "self" dello storage con "/disks", ad esempio:

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

Si espande

Molti comandi API supportano il parametro **expand**, che fornisce dettagli aggiuntivi sull'oggetto o sugli URL per gli oggetti correlati.

L'unico parametro di espansione comune è *expands*. La risposta contiene un elenco di tutte le espansioni specifiche disponibili per l'oggetto.

Ad esempio, quando si richiede quanto segue:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
L'API restituisce tutte le espansioni disponibili per l'oggetto come
segue:
```

```
{
    "id": "1247936",
      "self": "/rest/v1/assets/storages/1247936",
      "name": "amsprdclu01",
      "simpleName": "amsprdclu01",
      "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
      "ip": "10.64.0.132",
      "serialNumber": "1-80-000011",
      "model": "FAS3270,FAS6290",
      "vendor": "NetApp",
      "microcodeVersion": "8.1.3 clustered Data ONTAP",
      "capacity": {
        "description": "Storage Capacity",
        "unitType": "MB",
        "total": {
          "value": 8.23185105E8
        },
        "storagePools": {
          "value": 5.43220974E8
        }
      },
      "isActive": true,
      "createTime": "2013-05-07T16:52:21-0700",
      "family": "FAS3200,FAS6200",
      "managementUrl": null,
      "virtualizedType": "STANDARD",
      "protocols":
      [
        "NAS",
        "NFS",
        "CIFS",
        "FC",
        "ISCSI"
      ],
      "_expands": {
        "performance": {
          "url": "/rest/v1/assets/storages/1247936/performance",
          "name": "Performance Data"
        },
        "storageNodes": {
          "url": "/rest/v1/assets/storages/1247936/storageNodes",
          "name": "Storage Storage Nodes"
        },
        "storagePools": {
          "url": "/rest/v1/assets/storages/1247936/storagePools",
          "name": "Storage Storage Pools"
        },
        "storageResources": {
          "url": "/rest/v1/assets/storages/1247936/storageResources",
          "name": "Storage Storage Resources"
        },
        "internalVolumes": {
          "url": "/rest/v1/assets/storages/1247936/internalVolumes",
          "name": "Storage Internal Volumes"
        },
        "volumes": {
          "url": "/rest/v1/assets/storages/1247936/volumes",
          "name": "Storage Volumes"
        },
        "disks": {
          "url": "/rest/v1/assets/storages/1247936/disks",
          "name": "Disks"
        },
        "datasources": {
          "url": "/rest/v1/assets/storages/1247936/datasources",
          "name": "Storage Datasources"
        },
        "ports": {
          "url": "/rest/v1/assets/storages/1247936/ports",
          "name": "Storage Ports"
        },
        "annotations": {
          "url": "/rest/v1/assets/storages/1247936/annotations",
          "name": "Storage Annotations"
        },
        "qtrees": {
          "url": "/rest/v1/assets/storages/1247936/qtrees",
          "name": "Qtrees"
        },
```

Ogni espansione contiene dati, un URL o entrambi. Il parametro expand supporta attributi multipli e annidati, ad esempio:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Espandi consente di importare molti dati correlati in un'unica risposta.
NetApp consiglia di non richiedere troppe informazioni contemporaneamente,
poiché ciò potrebbe causare un calo delle prestazioni.
```

Per scoraggiare questo fenomeno, le richieste di raccolte di livello superiore non possono essere ampliate. Ad esempio, non è possibile richiedere l'espansione dei dati per tutti gli oggetti di archiviazione contemporaneamente. I client devono recuperare l'elenco degli oggetti e quindi scegliere oggetti specifici da espandere.

Dati sulle prestazioni

I dati sulle prestazioni vengono raccolti su più dispositivi come campioni separati. Ogni ora (impostazione predefinita), Data Infrastructure Insights aggrega e riepiloga i campioni di prestazioni.

L'API consente l'accesso sia ai campioni sia ai dati riepilogati. Per un oggetto con dati sulle prestazioni, un riepilogo delle prestazioni è disponibile come *expand=performance*. Le serie temporali della cronologia delle prestazioni sono disponibili tramite *expand=performance.history* annidato.

Esempi di oggetti Performance Data includono:

- Prestazioni di archiviazione
- StoragePoolPerformance
- Prestazioni portuali
- Prestazioni del disco

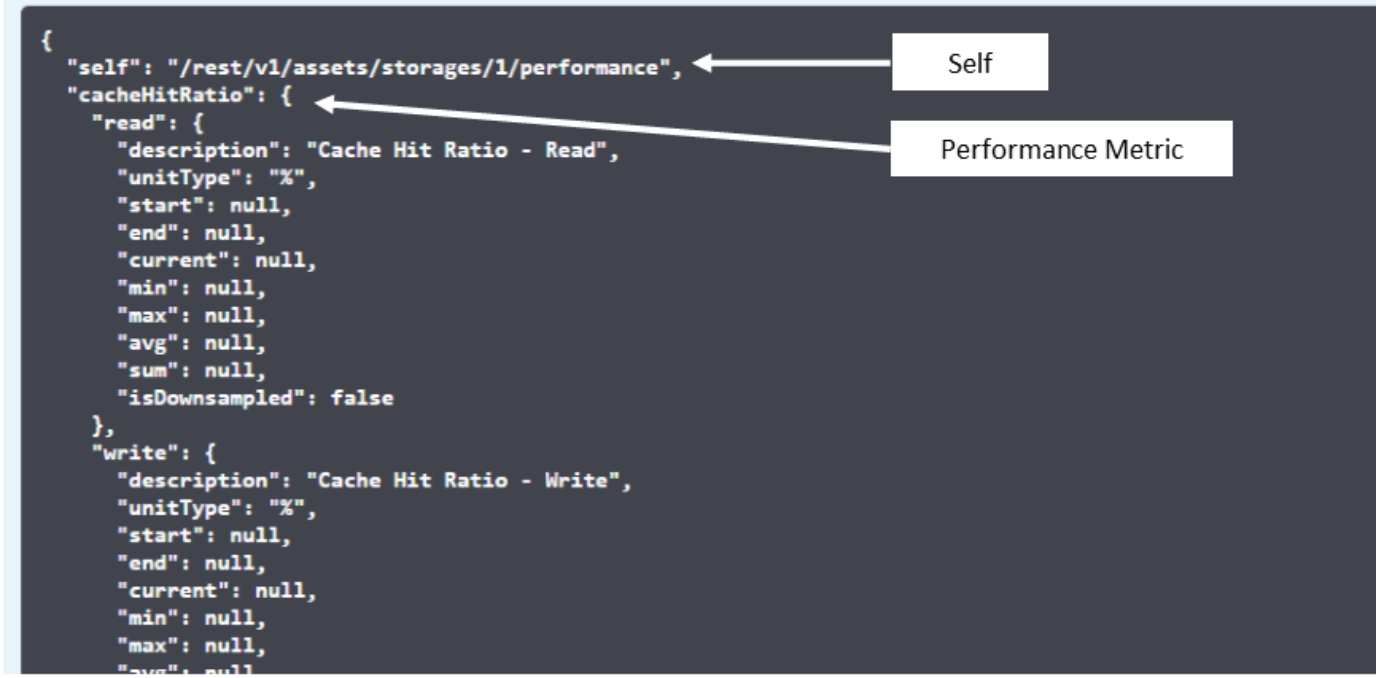
Una metrica delle prestazioni ha una descrizione e un tipo e contiene una raccolta di riepiloghi delle prestazioni. Ad esempio, Latenza, Traffico e Velocità.

Un riepilogo delle prestazioni contiene una descrizione, un'unità, un orario di inizio e di fine del campione e una raccolta di valori riepilogati (corrente, minimo, massimo, medio, ecc.) calcolati da un singolo contatore delle prestazioni in un intervallo di tempo (1 ora, 24 ore, 3 giorni e così via).

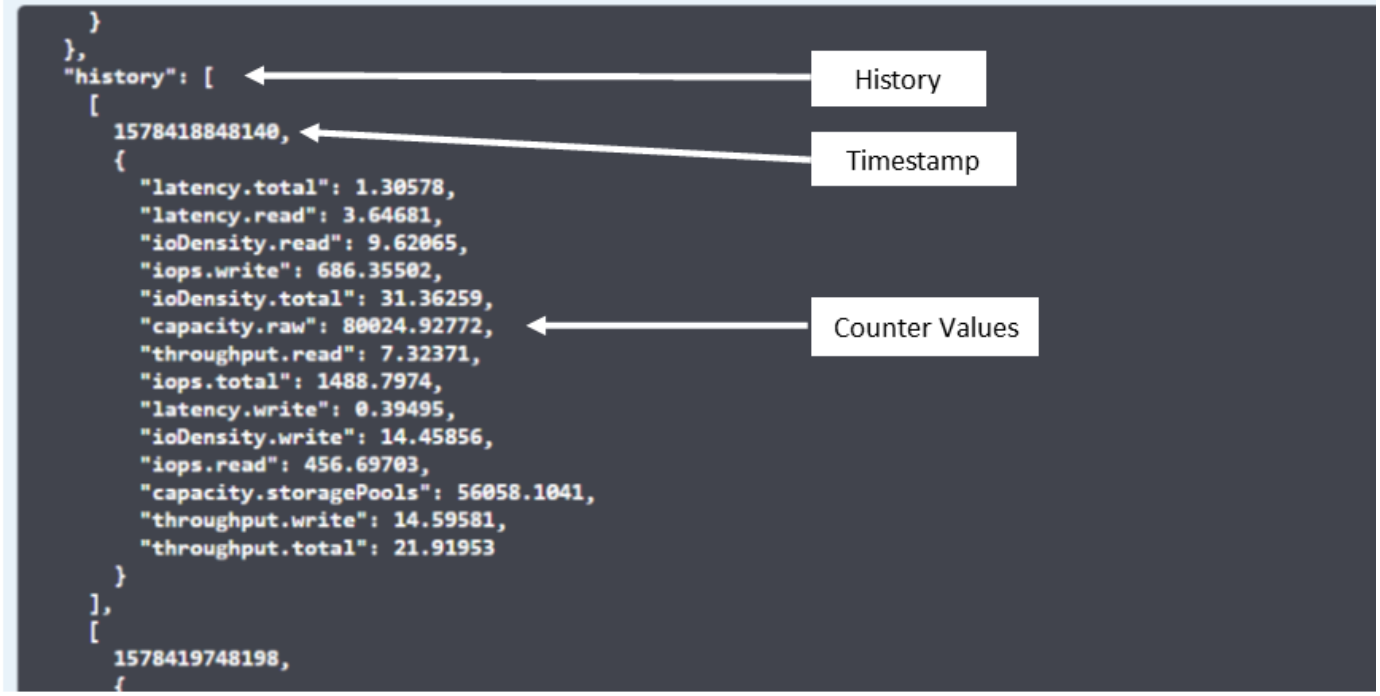
https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body



Response body



Il dizionario Performance Data risultante ha le seguenti chiavi:

- "self" è l'URL univoco dell'oggetto

- “cronologia” è l’elenco delle coppie di timestamp e la mappa dei valori dei contatori
- Ogni altra chiave del dizionario ("diskThroughput" e così via) è il nome di una metrica delle prestazioni.

Ogni tipo di oggetto dati sulle prestazioni ha un set univoco di metriche sulle prestazioni. Ad esempio, l’oggetto prestazioni della macchina virtuale supporta "diskThroughput" come metrica delle prestazioni. Ogni metrica delle prestazioni supportata appartiene a una determinata "performanceCategory" presentata nel dizionario delle metriche. Data Infrastructure Insights supporta diversi tipi di metriche delle prestazioni elencati più avanti in questo documento. Ogni dizionario di metriche di prestazione avrà anche il campo "descrizione", che è una descrizione leggibile da un essere umano di questa metrica di prestazione e un set di voci di conteggio riepilogative delle prestazioni.

Il contatore Riepilogo prestazioni è il riepilogo dei contatori delle prestazioni. Presenta valori aggregati tipici come minimo, massimo e medio per un contatore, nonché l’ultimo valore osservato, l’intervallo di tempo per i dati riepilogati, il tipo di unità per il contatore e le soglie per i dati. Solo le soglie sono facoltative; il resto degli attributi è obbligatorio.

Sono disponibili riepiloghi delle prestazioni per questi tipi di contatori:

- Leggi – Riepilogo delle operazioni di lettura
- Scrivi – Riepilogo delle operazioni di scrittura
- Totale – Riepilogo di tutte le operazioni. Potrebbe essere maggiore della semplice somma di lettura e scrittura e potrebbe includere altre operazioni.
- Totale massimo – Riepilogo di tutte le operazioni. Questo è il valore totale massimo nell’intervallo di tempo specificato.

Metriche delle prestazioni degli oggetti

L’API può restituire metriche dettagliate per gli oggetti nel tuo tenant, ad esempio:

- Metriche delle prestazioni di archiviazione quali IOPS (numero di richieste di input/output al secondo), latenza o throughput.
- Metriche delle prestazioni dello switch, come l’utilizzo del traffico, i dati BB Credit Zero o gli errori delle porte.

Vedi il"Documentazione API Swagger" per informazioni sulle metriche per ciascun tipo di oggetto.

Dati storici delle prestazioni

I dati storici vengono presentati nei dati sulle prestazioni come un elenco di coppie di mappe di timestamp e contatori.

I contatori cronologici vengono denominati in base al nome dell’oggetto metrica delle prestazioni. Ad esempio, l’oggetto prestazioni della macchina virtuale supporta "diskThroughput", quindi la mappa cronologica conterrà chiavi denominate "diskThroughput.read", "diskThroughput.write" e "diskThroughput.total".

Il timestamp è nel formato orario UNIX.

Di seguito è riportato un esempio di dati sulle prestazioni JSON per un disco:

```
"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
      "performanceCategory": "IOPS",
      "description": "Disk IOPS",
      "read": {
        "description": "Disk Read Iops",
        "unitType": "IO/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 1,
        "min": 0,
        "max": 6,
        "avg": 0.5532
      },
  […]
     "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
      }
    },
    "history":
    [
      [
        1399300412690,
        {
          "utilization.total": 12,
          "iops.total": 26,
          "iops.write": 22,
          "iops.read": 4,
          "throughput.read": 0,
          "utilization.read": 2.12,
          "throughput.total": 5,
          "utilization.write": 10.24,
          "throughput.write": 5
```


Oggetti con attributi di capacità

Gli oggetti con attributi di capacità utilizzano tipi di dati di base e CapacityItem per la rappresentazione.

CapacitàArticolo

CapacityItem è una singola unità logica di capacità. Ha "value" e "highThreshold" in unità definite dal suo oggetto padre. Supporta anche una mappa di ripartizione opzionale che spiega come viene costruito il valore della capacità. Ad esempio, la capacità totale di uno storagePool da 100 TB sarebbe un CapacityItem con un valore pari a 100. La ripartizione potrebbe mostrare 60 TB allocati per i "dati" e 40 TB per gli "snapshot".

Nota: "highThreshold" rappresenta le soglie definite dal sistema per le metriche corrispondenti, che un client può utilizzare per generare avvisi o segnali visivi sui valori che non rientrano negli intervalli configurati accettabili.

Di seguito è mostrata la capacità per StoragePool con più contatori di capacità:

Utilizzo della ricerca per cercare oggetti

L'API di ricerca è un semplice punto di accesso al sistema. L'unico parametro di input per l'API è una stringa in formato libero e il JSON risultante contiene un elenco categorizzato di risultati. I tipi sono tipi di asset diversi dall'inventario, come storage, host, dataStore e così via. Ogni tipo conterrebbe un elenco di oggetti del tipo che corrispondono ai criteri di ricerca.

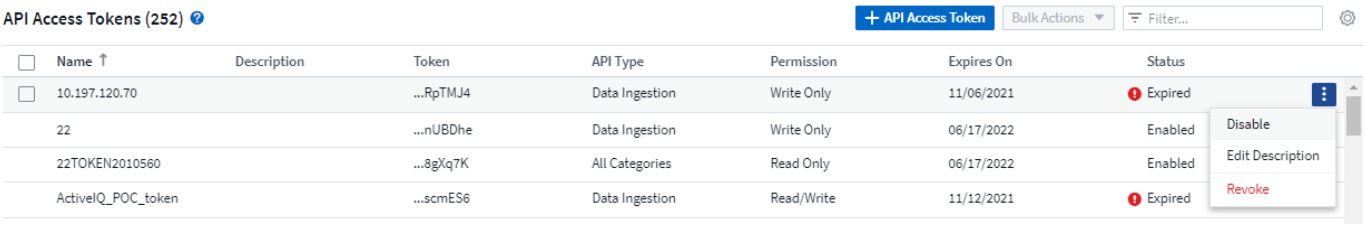
Data Infrastructure Insights è una soluzione estensibile (completamente aperta) che consente integrazioni con sistemi di orchestrazione, gestione aziendale, controllo delle modifiche e ticketing di terze parti, nonché integrazioni CMDB personalizzate.

L'API RESTful di Cloud Insight è un punto di integrazione primario che consente uno spostamento semplice ed efficace dei dati e consente agli utenti di accedere senza problemi ai propri dati.

Disabilitazione o revoca di un token API

Per disabilitare temporaneamente un token API, nella pagina dell'elenco dei token API, fare clic sul menu "tre punti" per l'API e selezionare *Disabilita*. È possibile riattivare il token in qualsiasi momento utilizzando lo stesso menu e selezionando *Abilita*.

Per rimuovere definitivamente un token API, seleziona "Revoca" dal menu. Non è possibile riattivare un token revocato; è necessario crearne uno nuovo.



Rotazione dei token di accesso API scaduti

I token di accesso API hanno una data di scadenza. Quando un token di accesso API scade, gli utenti devono generare un nuovo token (di tipo *Data Ingestion* con autorizzazioni di lettura/scrittura) e riconfigurare Telegraf per utilizzare il token appena generato anziché quello scaduto. Di seguito sono riportati i passaggi dettagliati per procedere.

Kubernetes

Si noti che questi comandi utilizzano lo spazio dei nomi predefinito "netapp-monitoring". Se hai impostato un tuo namespace, sostituiscilo in questi e in tutti i comandi e file successivi.

Nota: se hai installato la versione più recente NetApp Kubernetes Monitoring Operator e utilizzi un token di accesso API rinnovabile, i token in scadenza verranno automaticamente sostituiti da token di accesso API nuovi/aggiornati. Non è necessario eseguire manualmente i passaggi elencati di seguito.

- Crea un nuovo token API.
- Segui i passaggi per"Aggiornamento manuale" , selezionando il nuovo token API.

Nota: i clienti che gestiscono il proprio NetApp Kubernetes Monitoring Operator con uno strumento di gestione della configurazione, come Kustomize, possono seguire gli stessi passaggi per generare e scaricare un set aggiornato di YAML da inviare al proprio repository.

RHEL/CentOS e Debian/Ubuntu

- Modifica i file di configurazione di Telegraf e sostituisci tutte le istanze del vecchio token API con il nuovo token API.

```
 sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* Riavvia Telegraf.
```

```
sudo systemctl restart telegraf
```

Finestre

- Per ogni file di configurazione di Telegraf in *C:\Programmi\telegraf\telegraf.d*, sostituire tutte le istanze del vecchio token API con il nuovo token API.

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Riavvia Telegraf.

```
Stop-Service telegraf
Start-Service telegraf
```

Monitoraggio dell'ambiente

Revisione contabile

Per identificare le modifiche previste (per il monitoraggio) o impreviste (per la risoluzione dei problemi), è possibile visualizzare un audit trail degli eventi di sistema e delle attività degli utenti Data Infrastructure Insights .

Visualizzazione degli eventi verificati

Per visualizzare la pagina Audit, fare clic su **Amministrazione > Audit** nel menu. Viene visualizzata la pagina Audit, che fornisce i seguenti dettagli per ogni voce di audit:

- **Ora** - Data e ora dell'evento o dell'attività
- **Utente** - L'utente che ha avviato l'attività
- **Ruolo** - Il ruolo dell'utente in Data Infrastructure Insights (ospite, utente, amministratore)
- **IP** - L'indirizzo IP associato all'evento
- **Azione** - Tipo di attività, ad esempio Accedi, Crea, Aggiorna
- **Categoria** - La categoria di attività
- **Dettagli** - Dettagli dell'attività

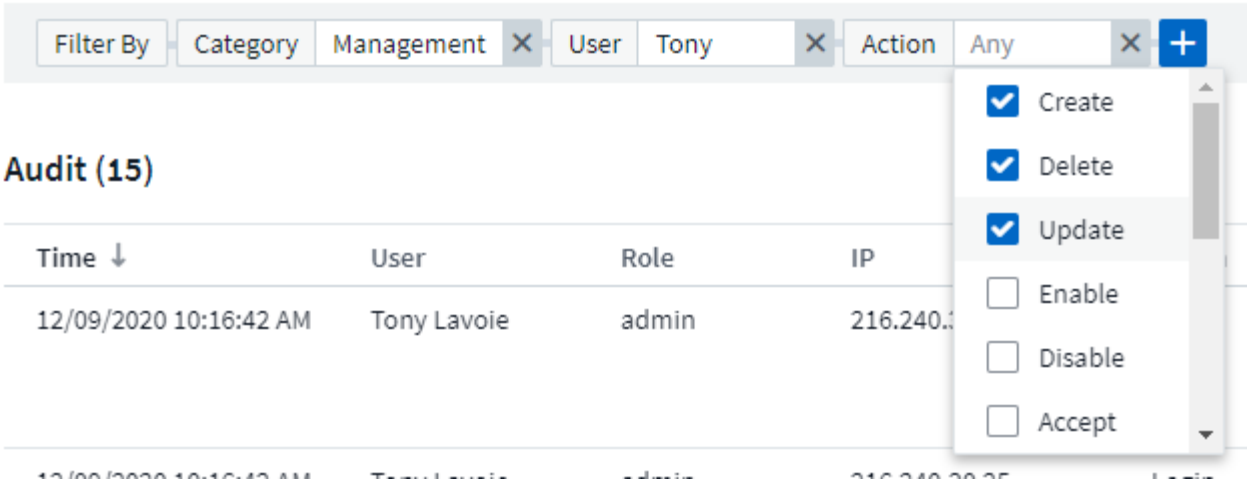
Visualizzazione delle voci di controllo

Esistono diversi modi per visualizzare le voci di controllo:

- È possibile visualizzare le voci di controllo scegliendo un periodo di tempo specifico (1 ora, 24 ore, 3 giorni, ecc.).
- È possibile modificare l'ordinamento delle voci in crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell'intestazione della colonna.

  Per impostazione predefinita, la tabella visualizza le voci in ordine temporale decrescente.

- È possibile utilizzare i campi filtro per visualizzare nella tabella solo le voci desiderate. Fare clic sul pulsante [+] per aggiungere ulteriori filtri.



Ulteriori informazioni sul filtraggio

Per affinare il filtro puoi utilizzare uno qualsiasi dei seguenti metodi:

Filtro	Cosa fa	Esempio	Risultato
* (Asterisco)	ti permette di cercare tutto	vol*rhel	restituisce tutte le risorse che iniziano con "vol" e finiscono con "rhel"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	BOS-PRD??-S12	restituisce BOS-PRD***12*** -S12, BOS-PRD***23***-S12 e così via
O	consente di specificare più entità	FAS2240 O CX600 O FAS3270	restituisce uno qualsiasi tra FAS2440, CX600 o FAS3270
NON	consente di escludere il testo dai risultati della ricerca	NON EMC*	restituisce tutto ciò che non inizia con "EMC"
Nessuno	cerca vuoto/NULL/Nessuno in qualsiasi campo in cui è selezionato	*Nessuno*	restituisce risultati in cui il campo di destinazione non è vuoto
Non *	come con *None* sopra, ma puoi anche usare questo modulo per cercare valori NULL nei campi *solo testo*	Non *	restituisce risultati in cui il campo di destinazione non è vuoto.
""	cerca una corrispondenza esatta	"NetApp*"	restituisce risultati contenenti la stringa letterale esatta *NetApp**

Se si racchiude una stringa di filtro tra virgolette doppie, Insight considera tutto ciò che si trova tra la prima e l'ultima virgoletta come una corrispondenza esatta. Tutti i caratteri speciali o gli operatori all'interno delle virgolette verranno trattati come valori letterali. Ad esempio, filtrando per "*" si otterranno risultati che sono un asterisco letterale; in questo caso l'asterisco non verrà trattato come un carattere jolly. Anche gli operatori OR e NOT verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

Eventi e azioni verificati

Gli eventi e le azioni controllati da Data Infrastructure Insights possono essere classificati nelle seguenti aree generali:

- **Account utente**: accesso, disconnessione, cambio ruolo, ecc.
- **Unità di acquisizione**: crea, elimina, ecc.

  Esempio: *Unità di acquisizione **AU-Boston-1** rimossa*.

- **Data Collector**: aggiungi, rimuovi, modifica, posticipa/riprendi, cambia unità di acquisizione, avvia/arresta, ecc.

  Esempio: *Datasource * FlexPod Lab* rimosso, fornitore * NetApp*, modello * ONTAP Data Management Software*, IP **192.168.106.5***.

- **Applicazione**: aggiungi, assegna a un oggetto, rimuovi, ecc.

  Esempio: *Volume interno **ocisedev:t1appSVM01:t1appFlexVol01** aggiunto all'applicazione **Test App***.

- **Annotazione**: aggiungi, assegna, rimuovi, azioni di regole di annotazione, modifiche del valore di annotazione, ecc.

  Esempio: *Valore di annotazione **Boston** aggiunto al tipo di annotazione **SalesOffice***.

- **Query**: aggiungi, rimuovi, ecc.

  Esempio: viene aggiunta la query **TL Sales Query**.

- **Monitor**: aggiungi, rimuovi, ecc.

  Esempio: Monitor *Aggr Size - CI Alerts Notifications Dev* aggiornato

- **Notifica**: modifica e-mail, ecc.

  Esempio: Destinatario *ci-alerts-notifications-dl* creato

Esportazione di eventi di audit

È possibile esportare i risultati della visualizzazione Audit in un file .CSV, che consentirà di analizzare i dati o di importarli in un'altra applicazione.

Passi

1. Nella pagina Audit, imposta l'intervallo di tempo desiderato e tutti i filtri che preferisci. Data Infrastructure Insights esporterà solo le voci di Audit che corrispondono al filtro e all'intervallo di tempo impostati.
2. Fare clic sul pulsante _Esporta_ in alto a destra della tabella.

Gli eventi di Audit visualizzati verranno esportati in un file .CSV, fino a un massimo di 10.000 righe.

Conservazione dei dati di audit

La quantità di tempo in cui Data Infrastructure Insights conserva i dati di audit dipende dall'abbonamento:

- Ambienti di prova: i dati di audit vengono conservati per 30 giorni

- Ambienti sottoscritti: i dati di audit vengono conservati per 1 anno più 1 giorno

Le voci di controllo più vecchie del periodo di conservazione vengono eliminate automaticamente. Non è richiesta alcuna interazione da parte dell'utente.

Le voci di controllo più vecchie del periodo di conservazione vengono eliminate automaticamente. Non è richiesta alcuna interazione da parte dell'utente.

Risoluzione dei problemi

Qui troverete suggerimenti per la risoluzione dei problemi con Audit.

Problema:	Prova questo:
Vedo messaggi di controllo che mi informano che un monitor è stato esportato.	L'esportazione di una configurazione di monitor personalizzata viene solitamente utilizzata dagli ingegneri NetApp durante lo sviluppo e il test di nuove funzionalità. Se non ti aspettavi di vedere questo messaggio, ti preghiamo di esaminare le azioni dell'utente indicato nell'azione verificata o di contattare l'assistenza.

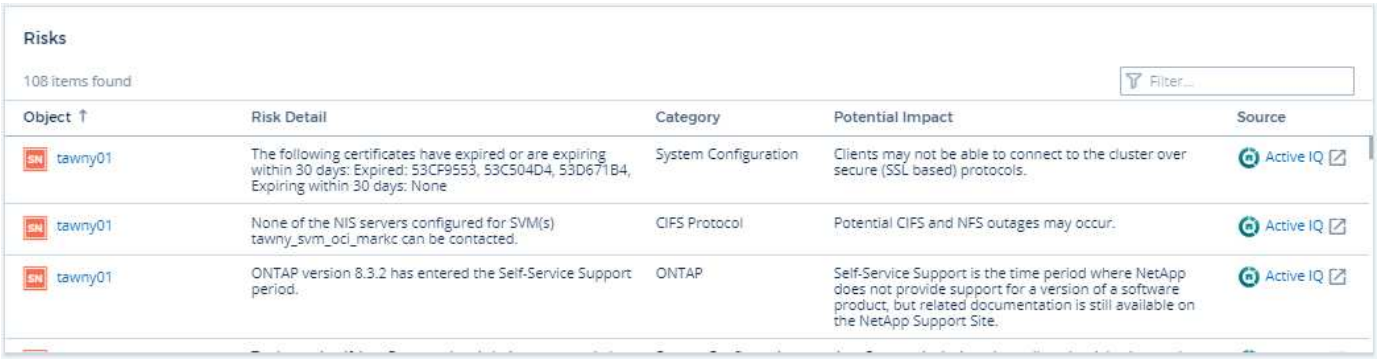
Digital Advisor Active IQ

NetApp"Digital Advisor Active IQ" (noto anche come Digital Advisor) fornisce una serie di visualizzazioni, analisi e altri servizi di supporto ai clienti NetApp per i loro sistemi hardware/software. I dati segnalati da Digital Advisor possono migliorare la risoluzione dei problemi di sistema e fornire informazioni utili per l'ottimizzazione e l'analisi predittiva dei tuoi dispositivi.

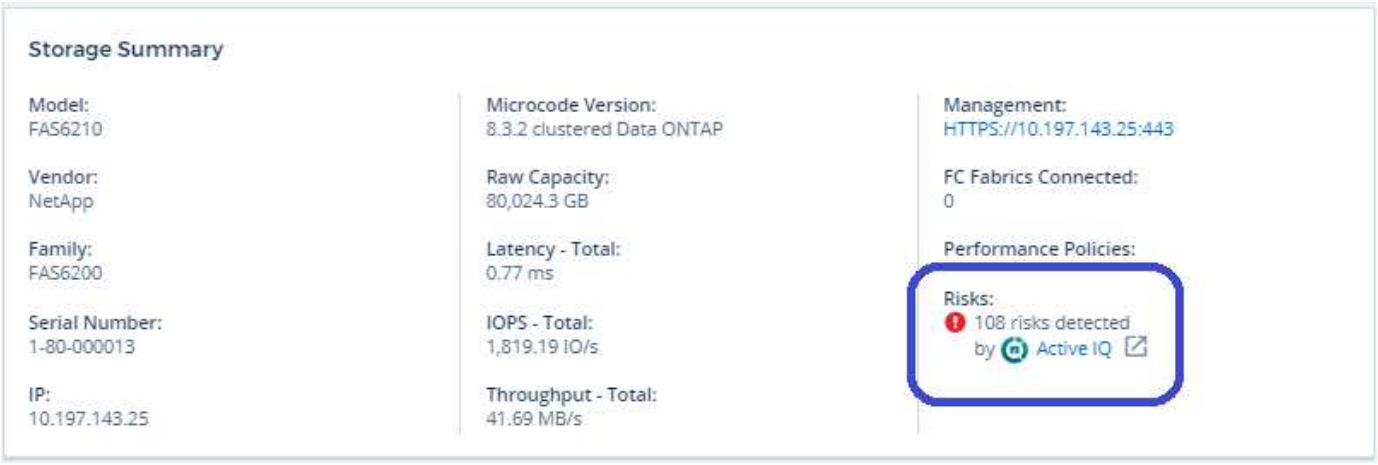
Data Infrastructure Insights raccoglie i **Rischi** per qualsiasi sistema di storage NetApp Clustered Data ONTAP monitorato e segnalato da Digital Advisor. I rischi segnalati per i sistemi di archiviazione vengono raccolti automaticamente da Data Infrastructure Insights come parte della raccolta dati da tali dispositivi. Per raccogliere informazioni sui rischi Digital Advisor , è necessario aggiungere il raccoglitore dati appropriato a Data Infrastructure Insights .

Data Infrastructure Insights non mostrerà i dati sui rischi per i sistemi ONTAP che non sono monitorati e segnalati da Digital Advisor.

I rischi segnalati sono mostrati in Data Infrastructure Insights nelle landing page delle risorse *storage* e *storage node*, nella tabella "Rischi". La tabella mostra i dettagli del rischio, la categoria di rischio e il potenziale impatto del rischio e fornisce anche un collegamento alla pagina Digital Advisor che riassume tutti i rischi per il nodo di archiviazione (è richiesto l'accesso all'account di supporto NetApp).



Un conteggio dei rischi segnalati viene visualizzato anche nel widget Riepilogo della landing page, con un collegamento alla pagina Digital Advisor appropriata. In una landing page di *archiviazione*, il conteggio è la somma dei rischi di tutti i nodi di archiviazione sottostanti.



Apertura della pagina Digital Advisor

Quando si fa clic sul collegamento a una pagina Digital Advisor , se non si è effettuato l'accesso al proprio account Digital Advisor , è necessario eseguire i seguenti passaggi per visualizzare la pagina Digital Advisor per il nodo di archiviazione.

1. Nel widget Riepilogo Data Infrastructure Insights o nella tabella Rischi, fare clic sul collegamento "Digital Advisor".
2. Sign in al tuo account di supporto NetApp . Verrai indirizzato direttamente alla pagina del nodo di archiviazione in Digital Advisor.

Ricerca dei rischi

In Data Infrastructure Insights, è possibile aggiungere la colonna **monitoring.count** a una query di archiviazione o di nodo di archiviazione. Se il risultato restituito include Digital Advisor- Sistemi di archiviazione monitorati, la colonna monitoring.count visualizzerà il numero di rischi per il sistema di archiviazione o il nodo.

Dashboard

È possibile creare widget (ad esempio grafici a torta, widget tabella, widget barra, widget colonna, widget grafico a dispersione e widget valore singolo) per visualizzare i rischi degli oggetti per l'archiviazione e i nodi di archiviazione per i sistemi NetApp Clustered Data ONTAP monitorati da Digital Advisor. È possibile selezionare "Rischi oggetto" come colonna o metrica in questi widget in cui l'oggetto di interesse è Storage o Storage Node.

Object Risks by Array

12 items found

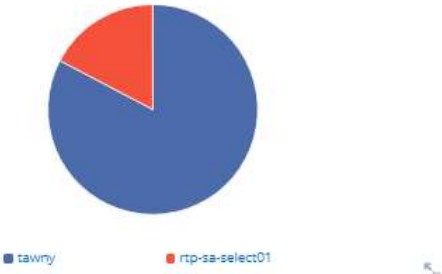
Name	Object Risks
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdsfc01	N/A
oci-3070-01	N/A

Object Risks by Node

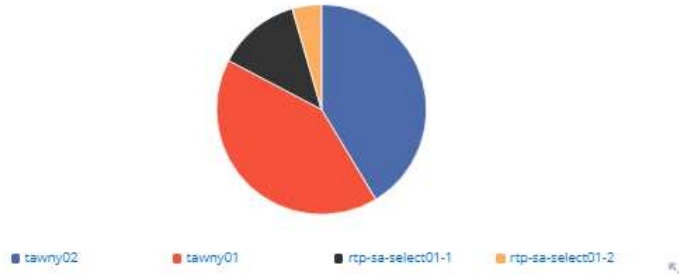
25 items found

Name	Object Risks
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A

Object Risks by Storage



Object Risks by Storage Node



Total Storage Risks

133.00

Object Risks

Sicurezza del carico di lavoro

Informazioni sulla sicurezza del carico di lavoro di archiviazione

Data Infrastructure Insights Storage Workload Security (in precedenza Cloud Secure) aiuta a proteggere i tuoi dati con informazioni fruibili sulle minacce interne. Fornisce visibilità e controllo centralizzati di tutti gli accessi ai dati aziendali negli ambienti cloud ibridi, per garantire il raggiungimento degli obiettivi di sicurezza e conformità.

Visibilità

Ottieni visibilità e controllo centralizzati dell'accesso degli utenti ai dati aziendali critici archiviati in sede o nel cloud.

Sostituire gli strumenti e i processi manuali che non riescono a fornire una visibilità tempestiva e accurata dell'accesso e del controllo dei dati. Workload Security funziona in modo esclusivo sia sui sistemi di archiviazione cloud che su quelli on-premise per fornirti avvisi in tempo reale sui comportamenti dannosi degli utenti.

Protezione

Proteggi i dati aziendali dall'uso improprio da parte di utenti malintenzionati o compromessi tramite l'apprendimento automatico avanzato e il rilevamento delle anomalie.

Ti avvisa di eventuali accessi anomali ai dati tramite apprendimento automatico avanzato e rilevamento di anomalie nel comportamento dell'utente.

Conformità

Garantisci la conformità aziendale verificando l'accesso dei dati utente ai dati aziendali critici archiviati in sede o nel cloud.

Iniziare

Introduzione alla sicurezza del carico di lavoro

Workload Security ti aiuta a monitorare l'attività degli utenti e a rilevare potenziali minacce alla sicurezza nel tuo ambiente di archiviazione. Prima di poter iniziare il monitoraggio, è necessario configurare agenti, raccoglitori di dati e servizi di directory per gettare le basi per un monitoraggio completo della sicurezza.

Il sistema Workload Security utilizza un agente per raccogliere i dati di accesso dai sistemi di archiviazione e le informazioni utente dai server Directory Services.

Prima di poter iniziare a raccogliere dati, è necessario configurare quanto segue:

Compito	Informazioni correlate

Configurare un agente	"Requisiti dell'agente" "Aggiungi agente"
Configurare un connettore di directory utente	"Aggiungi connettore directory utente"
Configurare i raccoglitori di dati	Fare clic su **Sicurezza del carico di lavoro > Collettori**. Fare clic sul collettore dati che si desidera configurare. Per informazioni sul collettore, consultare la sezione Riferimento del fornitore del Data Collector della documentazione.
Crea account utente	"Gestisci account utente"

Workload Security può essere integrato anche con altri strumenti. Per esempio,"vedi questa guida" sull'integrazione con Splunk.

Requisiti dell'agente di sicurezza del carico di lavoro

Distribuisci gli agenti Workload Security su server dedicati che soddisfano i requisiti minimi di sistema operativo, CPU, memoria e spazio su disco per garantire prestazioni ottimali di monitoraggio e rilevamento delle minacce. Questa guida specifica i requisiti hardware e di rete necessari prima di "installazione del Workload Security Agent", incluse le distribuzioni Linux supportate, le regole di connettività di rete e le indicazioni sul dimensionamento del sistema.

Componente	Requisiti Linux
Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti: * AlmaLinux 9.4 (64 bit) fino a 9.5 (64 bit), 10 (64 bit), incluso SELinux * CentOS Stream 9 (64 bit) * Debian 11 (64 bit), 12 (64 bit), incluso SELinux * OpenSUSE Leap 15.3 (64 bit) fino a 15.6 (64 bit) * Oracle Linux 8.10 (64 bit), 9.1 (64 bit) fino a 9.6 (64 bit), incluso SELinux * Red Hat Enterprise Linux 8.10 (64 bit), 9.1 (64 bit) fino a 9.6 (64 bit), 10 (64 bit), incluso SELinux * Rocky 9.4 (64 bit) fino a 9.6 (64 bit), incluso SELinux * SUSE Linux Enterprise Server Da 15 SP4 (64 bit) a 15 SP6 (64 bit), incluso SELinux * Ubuntu 20.04 LTS (64 bit), 22.04 LTS (64 bit), 24.04 LTS (64 bit) Su questo computer non deve essere in esecuzione nessun altro software a livello di applicazione. Si consiglia un server dedicato.
Comandi	Per l'installazione è necessario 'unzip'. Inoltre, per l'installazione, l'esecuzione degli script e la disinstallazione è necessario il comando 'sudo su –'.
processore	4 core della CPU
Memoria	16 GB di RAM

Componente	Requisiti Linux
Spazio disponibile su disco	Lo spazio su disco dovrebbe essere allocato in questo modo: /opt/netapp 36 GB (minimo 35 GB di spazio libero dopo la creazione del file system) Nota: si consiglia di allocare un po' di spazio su disco extra per consentire la creazione del file system. Assicurarsi che ci siano almeno 35 GB di spazio libero nel file system. Se /opt è una cartella montata da un archivio NAS, assicurarsi che gli utenti locali abbiano accesso a questa cartella. L'installazione dell'agente o del raccoglitore dati potrebbe non riuscire se gli utenti locali non dispongono dell'autorizzazione per questa cartella. Vedere"Risoluzione dei problemi" sezione per maggiori dettagli.
Rete	Connessione Ethernet da 100 Mbps a 1 Gbps, indirizzo IP statico, connettività IP a tutti i dispositivi e una porta obbligatoria per l'istanza di Workload Security (80 o 443).

Nota: l'agente Workload Security può essere installato nella stessa macchina di un'unità di acquisizione e/o di un agente Data Infrastructure Insights . Tuttavia, è buona norma installarli su macchine separate. Nel caso in cui siano installati sullo stesso computer, allocare lo spazio su disco come mostrato di seguito:

Spazio disponibile su disco	50-55 GB Per Linux, lo spazio su disco dovrebbe essere allocato in questo modo: /opt/netapp 25-30 GB /var/log/netapp 25 GB

Ulteriori raccomandazioni

- Si consiglia vivamente di sincronizzare l'ora sia sul sistema ONTAP che sulla macchina dell'agente utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

Regole di accesso alla rete cloud

Per ambienti di sicurezza del carico di lavoro con sede negli Stati Uniti:

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<nome_sito>.cs01.cloudinsights.netapp.com <nome_sito>.c01.cloudinsights.netapp.com <nome_sito>.c02.cloudinsights.netapp.com	Accesso alle Data Infrastructure Insights
TCP	443	Agente di sicurezza del carico di lavoro	agentlogin.cs01.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Per ambienti di sicurezza dei carichi di lavoro **con sede in Europa**:

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<nome_sito>.cs01-eu-1.cloudinsights.netapp.com <nome_sito>.c01-eu-1.cloudinsights.netapp.com <nome_sito>.c02-eu-1.cloudinsights.netapp.com	Accesso alle Data Infrastructure Insights
TCP	443	Agente di sicurezza del carico di lavoro	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Per ambienti di sicurezza del carico di lavoro basati su **APAC**:

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<nome_sito>.cs01-ap-1.cloudinsights.netapp.com <nome_sito>.c01-ap-1.cloudinsights.netapp.com <nome_sito>.c02-ap-1.cloudinsights.netapp.com	Accesso alle Data Infrastructure Insights
TCP	443	Agente di sicurezza del carico di lavoro	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Regole in-network

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	389 (LDAP) 636 (LDAP / start-tls)	Agente di sicurezza del carico di lavoro	URL del server LDAP	Connettiti a LDAP
TCP	443	Agente di sicurezza del carico di lavoro	Indirizzo IP di gestione del cluster o SVM (a seconda della configurazione del collettore SVM)	Comunicazione API con ONTAP

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	35000 - 55000	Indirizzi IP LIF dei dati SVM	Agente di sicurezza del carico di lavoro	Comunicazione da ONTAP al Workload Security Agent per gli eventi Fpolicy. Queste porte devono essere aperte verso il Workload Security Agent affinché ONTAP possa inviargli eventi, incluso qualsiasi firewall sul Workload Security Agent stesso (se presente). NOTA: non è necessario riservare **tutte** queste porte, ma le porte riservate a tale scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando circa 100 porte e di aumentarle se necessario.

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	35000-55000	IP di gestione del cluster	Agente di sicurezza del carico di lavoro	Comunicazione dall'IP di gestione del cluster ONTAP al Workload Security Agent per **eventi EMS**. Queste porte devono essere aperte verso il Workload Security Agent affinché ONTAP possa inviargli **eventi EMS**, incluso qualsiasi firewall sul Workload Security Agent stesso (se presente). NOTA: non è necessario riservare **tutte** queste porte, ma le porte riservate a tale scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando circa 100 porte e di aumentarle se necessario.
SSH	22	Agente di sicurezza del carico di lavoro	Gestione dei cluster	Necessario per il blocco degli utenti CIFS/SMB.

Dimensionamento del sistema

Vedi il"Verificatore del tasso di eventi" documentazione per informazioni sulle dimensioni.

Distribuisci agenti di sicurezza del carico di lavoro

Gli agenti Workload Security sono essenziali per monitorare l'attività degli utenti e rilevare potenziali minacce alla sicurezza nell'intera infrastruttura di storage. Questa guida fornisce istruzioni di installazione dettagliate, best practice per la gestione degli agenti (incluse le funzionalità di pausa/ripresa e blocco/sblocco) e requisiti di configurazione post-distribuzione. Prima di iniziare, assicurati che il tuo server agente soddisfi i requisiti "requisiti di sistema".

Prima di iniziare

- Il privilegio sudo è necessario per l'installazione, l'esecuzione di script e la disinstallazione.
- Durante l'installazione dell'agente, sulla macchina vengono creati un utente locale *cssys* e un gruppo

locale *cssys*. Se le impostazioni delle autorizzazioni non consentono la creazione di un utente locale e richiedono invece Active Directory, è necessario creare un utente con il nome utente *cssys* nel server Active Directory.

- Puoi leggere informazioni sulla sicurezza Data Infrastructure Insights"Qui" .

Migliori pratiche

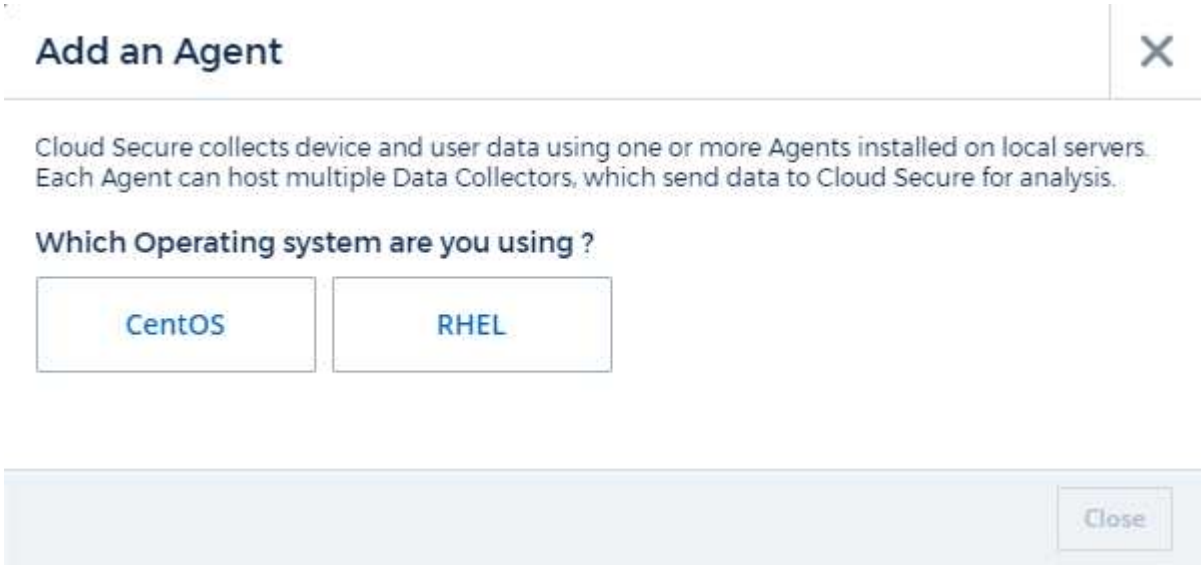
Prima di configurare l'agente Workload Security, tenere presente quanto segue.

Pausa e ripresa	Pausa: rimuove fpolicies da ONTAP. Solitamente utilizzato quando i clienti eseguono attività di manutenzione prolungate che potrebbero richiedere molto tempo, come riavvii di VM di agenti o sostituzioni di storage. Riprendi: aggiunge nuovamente fpolicies a ONTAP.
Fissare e sbloccare	Unpin recupera immediatamente la versione più recente (se disponibile) e aggiorna l'agente e il collettore. Durante questo aggiornamento, fpolicies si disconnetterà e si riconnetterà. Questa funzionalità è pensata per i clienti che desiderano controllare la tempistica degli aggiornamenti automatici. Vedi sotto peristruzioni per fissare/sganciare .
Approccio consigliato	Per configurazioni di grandi dimensioni, è consigliabile utilizzare Pin e Unpin anziché mettere in pausa i collettori. Non è necessario mettere in pausa e riprendere mentre si usa la funzione "blocca e sblocca". I clienti possono mantenere bloccati i propri agenti e collettori e, dopo aver ricevuto una notifica via e-mail relativa a una nuova versione, hanno una finestra di 30 giorni per aggiornare selettivamente gli agenti uno alla volta. Questo approccio riduce al minimo l'impatto della latenza sulle fpolicies e fornisce un maggiore controllo sul processo di aggiornamento.

Passaggi per installare l'agente

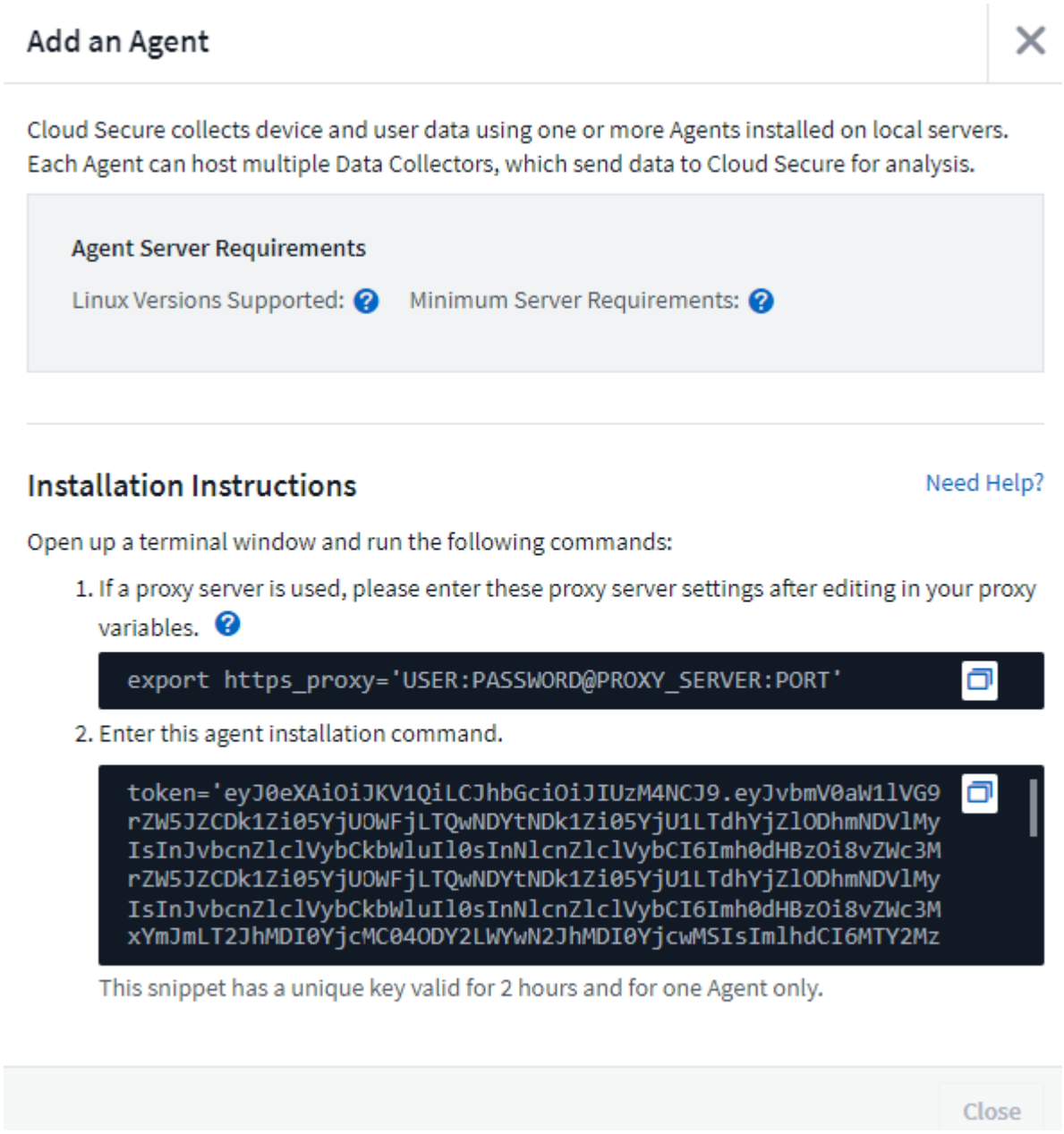
1. Accedi come amministratore o proprietario dell'account al tuo ambiente Workload Security.
2. Seleziona **Collezionisti > Agenti > +Agente**

   Il sistema visualizza la pagina Aggiungi un agente:



3. Verificare che il server agente soddisfi i requisiti minimi di sistema.

4. Per verificare che il server agente esegua una versione supportata di Linux, fare clic su *Versioni supportate (i)*.
5. Se la tua rete utilizza un server proxy, imposta i dettagli del server proxy seguendo le istruzioni nella sezione Proxy.



6. Fare clic sull'icona Copia negli Appunti per copiare il comando di installazione.
7. Eseguire il comando di installazione in una finestra del terminale.
8. Una volta completata correttamente l'installazione, il sistema visualizza il seguente messaggio:

Dopo aver finito

1. È necessario configurare un"Raccoglitore di directory utente" .
2. È necessario configurare uno o più Data Collector.

Configurazione di rete

Eseguire i seguenti comandi sul sistema locale per aprire le porte che verranno utilizzate da Workload Security. Se l'intervallo di porte presenta problemi di sicurezza, è possibile utilizzare un intervallo di porte inferiore, ad esempio *35000:35100*. Ogni SVM utilizza due porte.

Passi

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Segui i passaggi successivi in base alla tua piattaforma:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Esempio di output:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`(per CentOS 8)

Esempio di output:

```
35000-55000/tcp
```

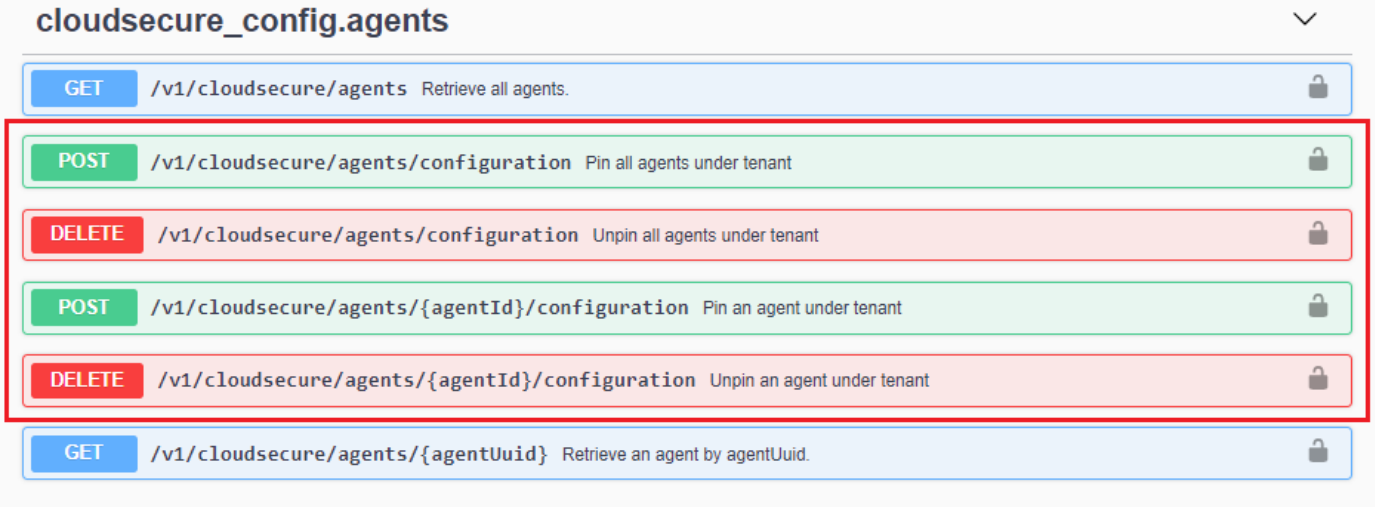
"Fissare" un agente alla versione corrente

Per impostazione predefinita, Data Infrastructure Insights Workload Security aggiorna automaticamente gli agenti. Alcuni clienti potrebbero voler sospendere l'aggiornamento automatico, lasciando un agente alla sua versione corrente finché non si verifica una delle seguenti situazioni:

- Il cliente riprende gli aggiornamenti automatici dell'agente.
- Sono trascorsi 30 giorni. Si noti che i 30 giorni iniziano il giorno dell'aggiornamento più recente dell'agente, non il giorno in cui l'agente è in pausa.

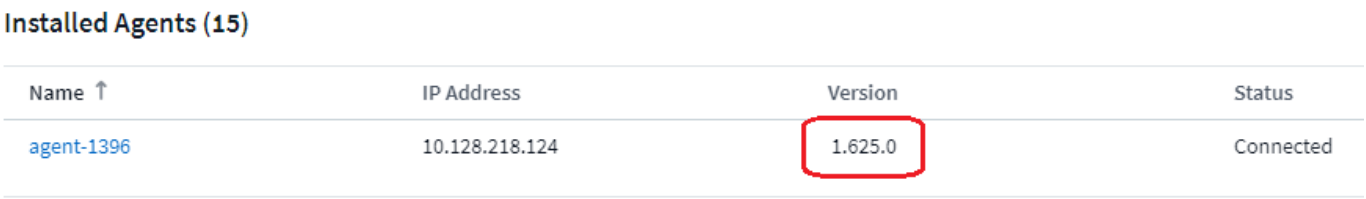
In ognuno di questi casi, l'agente verrà aggiornato al successivo aggiornamento di Workload Security.

Per sospendere o riprendere gli aggiornamenti automatici degli agenti, utilizzare le API *cloudsecure_config.agents*:



Tieni presente che potrebbero essere necessari fino a cinque minuti prima che l'azione di pausa o ripresa abbia effetto.

È possibile visualizzare le versioni correnti degli Agent nella pagina **Sicurezza del carico di lavoro > Collettori**, nella scheda **Agenti**.



Risoluzione dei problemi degli errori dell'agente

Nella tabella seguente sono descritti i problemi noti e le relative soluzioni.

Problema:	Risoluzione:
L'installazione dell'agente non riesce a creare la cartella /opt/netapp/cloudsecure/agent/logs/agent.log e il file install.log non fornisce informazioni rilevanti.	Questo errore si verifica durante il bootstrap dell'agente. L'errore non viene registrato nei file di registro perché si verifica prima dell'inizializzazione del logger. L'errore viene reindirizzato all'output standard ed è visibile nel registro del servizio utilizzando `journalctl -u cloudsecure-agent.service` comando. Questo comando può essere utilizzato per risolvere ulteriormente il problema. est
L'installazione dell'agente fallisce con il messaggio "Questa distribuzione Linux non è supportata". Uscita dall'installazione.	Questo errore viene visualizzato quando si tenta di installare l'agente su un sistema non supportato. Vedere "Requisiti dell'agente" .

Problema:	Risoluzione:
L'installazione dell'agente non è riuscita con l'errore: "-bash: unzip: comando non trovato"	Installa unzip e poi esegui nuovamente il comando di installazione. Se Yum è installato sul computer, prova "yum install unzip" per installare il software di decompressione. Dopodiché, copia nuovamente il comando dall'interfaccia utente di installazione dell'agente e incollalo nella CLI per eseguire nuovamente l'installazione.
L'agente è stato installato ed è in esecuzione. Tuttavia l'agente si è fermato all'improvviso.	Eseguire l'SSH sulla macchina dell'agente. Controllare lo stato del servizio agente tramite `sudo systemctl status cloudsecure-agent.service` . 1. Controllare se nei registri viene visualizzato il messaggio "Impossibile avviare il servizio daemon Workload Security". 2. Verificare se l'utente cssys esiste o meno nella macchina dell'agente. Eseguire i seguenti comandi uno alla volta con i permessi di root e verificare se l'utente e il gruppo cssys esistono. `sudo id cssys` `sudo groups cssys` 3. Se non ne esiste nessuno, è possibile che un criterio di monitoraggio centralizzato abbia eliminato l'utente cssys. 4. Creare manualmente l'utente e il gruppo cssys eseguendo i seguenti comandi. `sudo useradd cssys` `sudo groupadd cssys` 5. Successivamente riavviare il servizio agente eseguendo il seguente comando: `sudo systemctl restart cloudsecure-agent.service` 6. Se il problema persiste, controlla le altre opzioni di risoluzione dei problemi.
Impossibile aggiungere più di 50 raccoglitori di dati a un agente.	È possibile aggiungere solo 50 raccoglitori di dati a un agente. Può trattarsi di una combinazione di tutti i tipi di collettori, ad esempio Active Directory, SVM e altri collettori.
L'interfaccia utente mostra che l'agente è nello stato NOT_CONNECTED.	Passaggi per riavviare l'agente. 1. Eseguire l'SSH sulla macchina dell'agente. 2. Successivamente riavviare il servizio agente eseguendo il seguente comando: `sudo systemctl restart cloudsecure-agent.service` 3. Controllare lo stato del servizio agente tramite `sudo systemctl status cloudsecure-agent.service` . 4. L'agente dovrebbe passare allo stato CONNESSO.
L'agente VM si trova dietro il proxy Zscaler e l'installazione dell'agente non riesce. A causa dell'ispezione SSL del proxy Zscaler, i certificati di sicurezza del carico di lavoro vengono presentati così come sono firmati dalla CA Zscaler, quindi l'agente non si fida della comunicazione.	Disabilitare l'ispezione SSL nel proxy Zscaler per l'URL *.cloudinsights.netapp.com. Se Zscaler esegue l'ispezione SSL e sostituisce i certificati, Workload Security non funzionerà.

Problema:	Risoluzione:
Durante l’installazione dell’agente, l’installazione si blocca dopo la decompressione.	Il comando "chmod 755 -Rf" non funziona. Il comando fallisce quando il comando di installazione dell’agente viene eseguito da un utente sudo non root che ha file nella directory di lavoro, appartenenti a un altro utente, e le autorizzazioni di tali file non possono essere modificate. A causa del comando chmod non riuscito, il resto dell’installazione non viene eseguito. 1. Crea una nuova directory denominata “cloudsecure”. 2. Vai a quella directory. 3. Copia e incolla il comando di installazione completo “token=…… … ./cloudsecure-agent-install.sh" e premi Invio. 4. L’installazione dovrebbe poter procedere.
Se l’agente non riesce ancora a connettersi a Saas, aprire un caso con il supporto NetApp . Fornire il numero di serie Data Infrastructure Insights per aprire un caso e allegare i registri al caso come indicato.	Per allegare i registri alla custodia: 1. Eseguire lo script seguente con i permessi di root e condividere il file di output (cloudsecure-agent-symptoms.zip). a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Eseguire i seguenti comandi uno per uno con i permessi di root e condividere l’output. a. id cssys b. groups cssys c. cat /etc/os-release
Lo script cloudsecure-agent-symptom-collector.sh non riesce e restituisce il seguente errore. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Raccolta del registro di servizio Raccolta dei registri delle applicazioni Raccolta delle configurazioni degli agenti Acquisizione di uno snapshot dello stato del servizio Acquisizione di uno snapshot della struttura delle directory degli agenti ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: riga 52: zip: comando non trovato ERRORE: Impossibile creare /tmp/cloudsecure-agent-symptoms.zip	Lo strumento Zip non è installato. Installare lo strumento zip eseguendo il comando “yum install zip”. Quindi eseguire nuovamente cloudsecure-agent-symptom-collector.sh.
L’installazione dell’agente fallisce con useradd: impossibile creare la directory /home/cssys	Questo errore può verificarsi se la directory di accesso dell’utente non può essere creata in /home, a causa della mancanza di autorizzazioni. La soluzione alternativa sarebbe quella di creare l’utente cssys e aggiungere manualmente la sua directory di accesso utilizzando il seguente comando: *sudo useradd user_name -m -d HOME_DIR* -m : crea la directory home dell’utente se non esiste. -d: il nuovo utente viene creato utilizzando HOME_DIR come valore per la directory di accesso dell’utente. Ad esempio, *sudo useradd cssys -m -d /cssys*, aggiunge un utente *cssys* e crea la sua directory di accesso nella root.

Problema:	Risoluzione:
L'agente non è in esecuzione dopo l'installazione. *Systemctl status cloudsecure-agent.service* mostra quanto segue: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Servizio Daemon dell'agente di sicurezza del carico di lavoro Caricato: caricato (/usr/lib/systemd/system/cloudsecure-agent.service; abilitato; preimpostazione del fornitore: disabilitato) Attivo: attivazione (riavvio automatico) (Risultato: codice di uscita) da mar 2021-08-03 21:12:26 PDT; 2s fa Processo: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (codice=uscito stato=126) PID principale: 25889 (codice=uscito, stato=126), 03 ago 21:12:26 demo systemd[1]: cloudsecure-agent.service: processo principale uscito, codice=uscito, stato=126/n/d 03 ago 21:12:26 demo systemd[1]: l'unità cloudsecure-agent.service è entrata in stato di errore. 03 ago 21:12:26 demo systemd[1]: cloudsecure-agent.service non riuscito.	Questa operazione potrebbe non riuscire perché l'utente *cssys* potrebbe non avere l'autorizzazione per l'installazione. Se /opt/netapp è un mount NFS e se l'utente *cssys* non ha accesso a questa cartella, l'installazione non riuscirà. *cssys* è un utente locale creato dal programma di installazione di Workload Security che potrebbe non avere l'autorizzazione per accedere alla condivisione montata. È possibile verificarlo provando ad accedere a /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent utilizzando l'utente *cssys*. Se restituisce "Autorizzazione negata", l'autorizzazione all'installazione non è presente. Invece di una cartella montata, installa su una directory locale della macchina.
Inizialmente l'agente era connesso tramite un server proxy e il proxy è stato impostato durante l'installazione dell'agente. Ora il server proxy è cambiato. Come si può modificare la configurazione proxy dell'agente?	È possibile modificare agent.properties per aggiungere i dettagli del proxy. Seguire questi passaggi: 1. Passare alla cartella contenente il file delle proprietà: cd /opt/netapp/cloudsecure/conf 2. Utilizzando il tuo editor di testo preferito, apri il file *agent.properties* per modificarlo. 3. Aggiungere o modificare le seguenti righe: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Salva il file. 5. Riavviare l'agente: sudo systemctl restart cloudsecure-agent.service

Eliminazione di un agente di sicurezza del carico di lavoro

Quando si elimina un Workload Security Agent, è necessario eliminare prima tutti i raccoglitori di dati associati all'agente.

Eliminazione di un agente

L'eliminazione di un agente comporta l'eliminazione di tutti i Data Collector associati all'agente. Se si prevede di configurare i raccoglitori dati con un agente diverso, è necessario creare un backup delle configurazioni del raccoglitore dati prima di eliminare l'agente.

Prima di iniziare

1. Assicurarsi che tutti i raccoglitori di dati associati all'agente vengano eliminati dal portale Workload Security.

   Nota: ignorare questo passaggio se tutti i collettori associati sono nello stato STOPPED.

Passaggi per eliminare un agente:

1. Accedi tramite SSH alla VM dell'agente ed esegui il seguente comando. Quando richiesto, immettere "y" per continuare.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Fare clic su **Sicurezza del carico di lavoro > Collettori > Agenti**

   Il sistema visualizza l'elenco degli agenti configurati.

3. Fare clic sul menu delle opzioni per l'agente che si desidera eliminare.
4. Fare clic su **Elimina**.

   Il sistema visualizza la pagina **Elimina agente**.

5. Fare clic su **Elimina** per confermare l'eliminazione.

Configurazione di un raccoglitore di directory utente di Active Directory (AD)

Workload Security può essere configurato per raccogliere gli attributi utente dai server Active Directory.

Prima di iniziare

- Per eseguire questa attività, devi essere un amministratore di Data Infrastructure Insights o un proprietario dell'account.
- È necessario disporre dell'indirizzo IP del server che ospita il server Active Directory.
- Prima di configurare un connettore Directory utente, è necessario configurare un agente.

Passaggi per configurare un raccoglitore di directory utente

1. Nel menu Sicurezza del carico di lavoro, fare clic su: **Collector > User Directory Collector > + User Directory Collector** e selezionare **Active Directory**

   Il sistema visualizza la schermata Aggiungi directory utente.

Configurare User Directory Collector inserendo i dati richiesti nelle seguenti tabelle:

Nome	Descrizione
Nome	Nome univoco per la directory utente. Ad esempio *GlobalADCollector*
Agente	Seleziona un agente configurato dall'elenco
IP del server/nome di dominio	Indirizzo IP o nome di dominio completo (FQDN) del server che ospita Active Directory

Nome della foresta	Livello foresta della struttura delle directory. Il nome della foresta consente entrambi i seguenti formati: *x.y.z* ⇒ nome di dominio diretto così come è presente sulla SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nomi distinti relativi [Esempio: DC=hq,DC= companyname,DC=com] Oppure puoi specificare come segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [per filtrare in base a OU engineering specifica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [per ottenere solo un utente specifico con <username> da OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [per ottenere tutti gli utenti Acrobat all'interno degli utenti di quell'organizzazione] Sono supportati anche i domini Active Directory attendibili.
Associa DN	Utente autorizzato a effettuare ricerche nella directory. Ad esempio: *username@companyname.com* oppure *username@domainname.com* Inoltre, è richiesta l'autorizzazione di sola lettura del dominio. L'utente deve essere membro del gruppo di sicurezza *Controller di dominio di sola lettura*.
Password BIND	Password del server di directory (ovvero password per il nome utente utilizzato in Bind DN)
Protocollo	ldap, ldaps, ldap-start-tls
porti	Seleziona la porta

Immettere i seguenti attributi obbligatori del Directory Server se i nomi degli attributi predefiniti sono stati modificati in Active Directory. Nella maggior parte dei casi i nomi di questi attributi *non* vengono modificati in Active Directory, nel qual caso è possibile procedere semplicemente con il nome di attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome da visualizzare	nome
SID	oggetti
Nome utente	sAMAccountName

Fare clic su Includi attributi facoltativi per aggiungere uno qualsiasi dei seguenti attributi:

Attributi	Nome attributo nel server directory
Indirizzo e-mail	posta
Numero di telefono	numero di telefono
Ruolo	titolo
Paese	co
Stato	stato

Dipartimento	dipartimento
Foto	miniatura della foto
ManagerDN	manager
Gruppi	membroDi

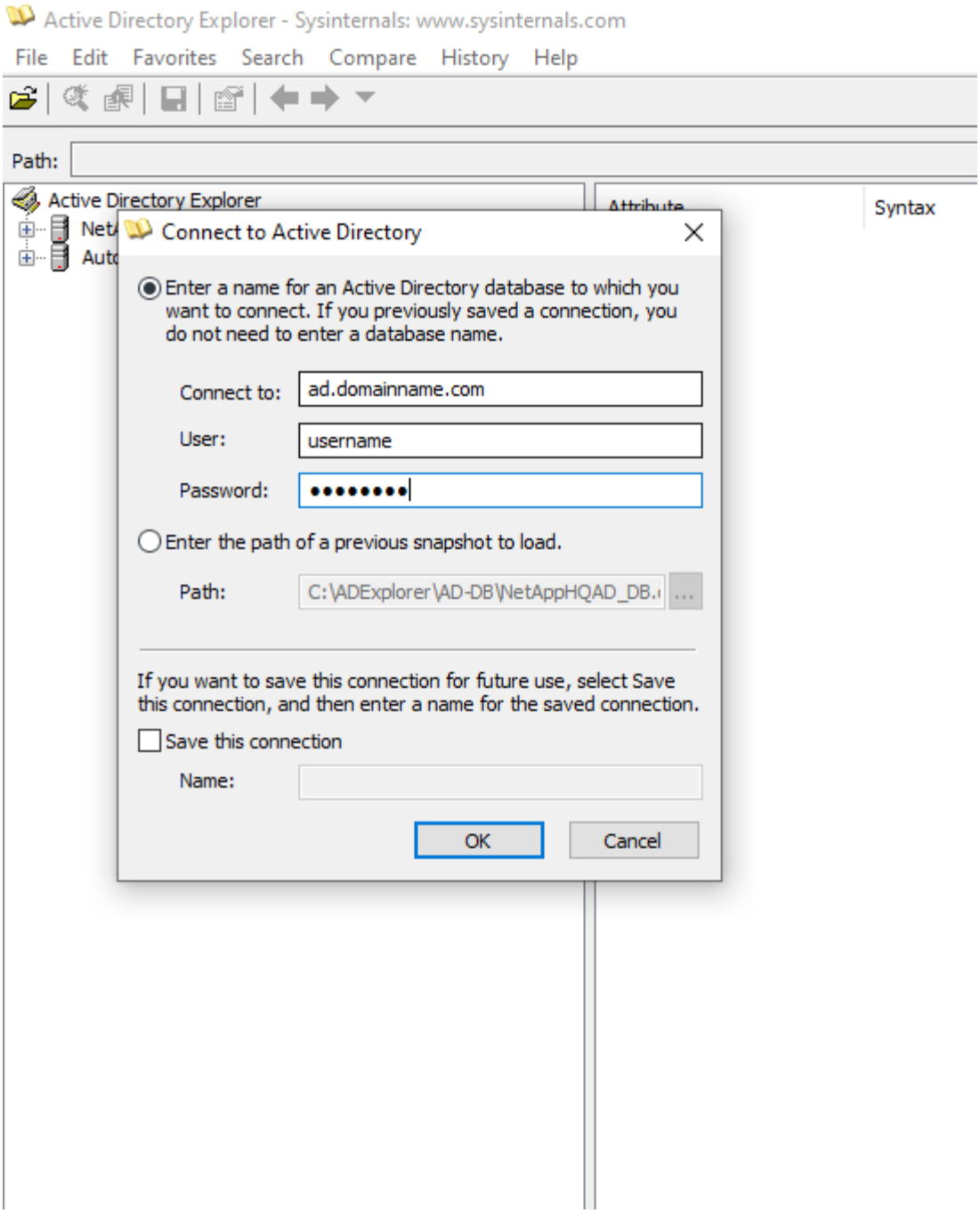
Test della configurazione del raccoglitore di directory utente

È possibile convalidare le autorizzazioni utente e le definizioni degli attributi LDAP utilizzando le seguenti procedure:

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP di Workload Security:

```
ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
389 -D Administrator@netapp.com -W
```

- Utilizzare AD Explorer per navigare in un database AD, visualizzare le proprietà e gli attributi degli oggetti, visualizzare le autorizzazioni, visualizzare lo schema di un oggetto, eseguire ricerche sofisticate che è possibile salvare e rieseguire.
  - Installare"Esploratore AD" su qualsiasi macchina Windows in grado di connettersi al server AD.
  - Connettersi al server AD utilizzando il nome utente/password del server della directory AD.



Risoluzione dei problemi relativi agli errori di configurazione del raccoglitore directory utente

Nella tabella seguente vengono descritti i problemi noti e le relative soluzioni che possono verificarsi durante la configurazione del collettore:

Problema:	Risoluzione:
L'aggiunta di un connettore Directory utente genera lo stato "Errore". L'errore dice: "Credenziali non valide fornite per il server LDAP".	Nome utente o password forniti non corretti. Modifica e fornisci il nome utente e la password corretti.

Problema:	Risoluzione:
L’aggiunta di un connettore Directory utente genera lo stato "Errore". L’errore dice: "Impossibile ottenere l’oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome foresta".	Nome foresta fornito errato. Modifica e fornisci il nome corretto della foresta.
Gli attributi facoltativi dell’utente di dominio non vengono visualizzati nella pagina Profilo utente di Workload Security.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. Modifica e fornisci i nomi corretti degli attributi facoltativi.
Il raccoglitore dati è in stato di errore con "Impossibile recuperare gli utenti LDAP. Motivo dell’errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore cliccando sul pulsante *Riavvia*.
L’aggiunta di un connettore Directory utente genera lo stato "Errore".	Assicurati di aver fornito valori validi per i campi obbligatori (Server, nome foresta, DN di associazione, password di associazione). Assicurarsi che l’input bind-DN sia sempre fornito come 'Administrator@<domain_forest_name>' o come account utente con privilegi di amministratore di dominio.
L’aggiunta di un connettore Directory utente determina lo stato "RITIRO". Mostra l’errore "Impossibile definire lo stato del collettore, motivo per cui il comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] non è riuscito a causa di java.net.ConnectionException:Connessione rifiutata."	IP o FQDN non corretti forniti per il server AD. Modifica e fornisci l’indirizzo IP o il nome di dominio completo (FQDN) corretto.
L’aggiunta di un connettore Directory utente genera lo stato "Errore". L’errore dice: "Impossibile stabilire la connessione LDAP".	IP o FQDN non corretti forniti per il server AD. Modifica e fornisci l’indirizzo IP o il nome di dominio completo (FQDN) corretto.
L’aggiunta di un connettore Directory utente genera lo stato "Errore". L’errore dice: "Impossibile caricare le impostazioni. Motivo: la configurazione dell’origine dati presenta un errore. Motivo specifico: /connector/conf/application.conf: 70: ldap.ldap-port ha il tipo STRING anziché NUMBER”	Valore non corretto per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server AD.
Ho iniziato con gli attributi obbligatori e ha funzionato. Dopo aver aggiunto quelli facoltativi, i dati degli attributi facoltativi non vengono recuperati da AD.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. Modifica e fornisci il nome corretto dell’attributo obbligatorio o facoltativo.
Dopo aver riavviato il collector, quando avverrà la sincronizzazione AD?	La sincronizzazione AD avverrà immediatamente dopo il riavvio del collector. Ci vorranno circa 15 minuti per recuperare i dati di circa 300.000 utenti e i dati vengono aggiornati automaticamente ogni 12 ore.

Problema:	Risoluzione:
I dati utente vengono sincronizzati da AD a CloudSecure. Quando verranno eliminati i dati?	In caso di mancato aggiornamento, i dati dell'utente vengono conservati per 13 mesi. Se l'inquilino viene eliminato, anche i dati verranno eliminati.
Il connettore della directory utente genera lo stato "Errore". "Il connettore è in stato di errore. Nome del servizio: usersLdap. Motivo dell'errore: impossibile recuperare gli utenti LDAP. Motivo dell'errore: 80090308: LdapErr: DSID-0C090453, commento: errore AcceptSecurityContext, dati 52e, v3839"	Nome foresta fornito errato. Per informazioni su come fornire il nome corretto della foresta, vedere sopra.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Molto probabilmente ciò è dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare lo specifico raccoglitore di Active Directory che recupera le informazioni dell'utente da Active Directory. 2. Si noti che tra gli attributi facoltativi è presente un campo denominato "Numero di telefono" mappato all'attributo di Active Directory "telephonenumber". 4. Ora, utilizzare lo strumento Active Directory Explorer come descritto sopra per esplorare Active Directory e visualizzare il nome corretto dell'attributo. 3. Assicurarsi che in Active Directory sia presente un attributo denominato "numero di telefono" che contenga effettivamente il numero di telefono dell'utente. 5. Supponiamo che in Active Directory sia stato modificato in "numero di telefono". 6. Quindi modifica il raccoglitore CloudSecure User Directory. Nella sezione degli attributi facoltativi, sostituire 'telephonenumber' con 'phonenumber'. 7. Salvare il raccoglitore di Active Directory, il raccoglitore verrà riavviato e otterrà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è abilitato sul server Active Directory (AD), Workload Security User Directory Collector non può connettersi al server AD.	Disattivare la crittografia del server AD prima di configurare un User Directory Collector. Una volta recuperati, i dati dell'utente rimarranno disponibili per 13 mesi. Se il server AD viene disconnesso dopo aver recuperato i dettagli dell'utente, gli utenti appena aggiunti in AD non verranno recuperati. Per effettuare nuovamente il recupero, il raccoglitore di directory utente deve essere connesso ad AD.
I dati di Active Directory sono presenti in CloudInsights Security. Vuoi eliminare tutte le informazioni utente da CloudInsights.	Non è possibile eliminare SOLO le informazioni utente di Active Directory da CloudInsights Security. Per eliminare l'utente, è necessario eliminare l'intero tenant.

Configurazione di un server di raccolta directory LDAP

È possibile configurare Workload Security per raccogliere gli attributi utente dai server della directory LDAP.

Prima di iniziare

- Per eseguire questa attività, devi essere un amministratore di Data Infrastructure Insights o un proprietario dell'account.
- È necessario disporre dell'indirizzo IP del server che ospita il server della directory LDAP.
- Prima di configurare un connettore di directory LDAP, è necessario configurare un agente.

Passaggi per configurare un raccoglitore di directory utente

1. Nel menu Sicurezza del carico di lavoro, fare clic su: **Collector > User Directory Collector > + User Directory Collector** e selezionare **LDAP Directory Server**

   Il sistema visualizza la schermata Aggiungi directory utente.

Configurare User Directory Collector inserendo i dati richiesti nelle seguenti tabelle:

Nome	Descrizione
Nome	Nome univoco per la directory utente. Ad esempio *GlobalLDAPCollector*
Agente	Seleziona un agente configurato dall'elenco
IP del server/nome di dominio	Indirizzo IP o nome di dominio completo (FQDN) del server che ospita il server di directory LDAP
Base di ricerca	Base di ricerca del server LDAP La base di ricerca consente entrambi i seguenti formati: *x.y.z* ⇒ nome di dominio diretto così come è presente sul tuo SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nomi distinti relativi [Esempio: DC=hq,DC= companyname,DC=com] Oppure puoi specificare come segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [per filtrare in base a OU engineering specifica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [per ottenere solo un utente specifico con <username> da OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [per ottenere tutti gli utenti Acrobat all'interno degli utenti di quell'organizzazione]
Associa DN	Utente autorizzato a effettuare ricerche nella directory. Ad esempio: uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=c ompanyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company ,dc=com per un utente john@dorp.company.com. dorp.company.com
--conti	--utenti
--Giovanni	--anna
Password BIND	Password del server di directory (ovvero password per il nome utente utilizzato in Bind DN)

Protocollo	ldap, ldaps, ldap-start-tls
porti	Seleziona la porta

Immettere i seguenti attributi obbligatori del Directory Server se i nomi degli attributi predefiniti sono stati modificati nel Directory Server LDAP. Nella maggior parte dei casi i nomi di questi attributi non vengono modificati in LDAP Directory Server, nel qual caso è possibile procedere semplicemente con il nome dell'attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome da visualizzare	nome
UNIXID	numero uid
Nome utente	fluido

Fare clic su Includi attributi facoltativi per aggiungere uno qualsiasi dei seguenti attributi:

Attributi	Nome attributo nel server directory
Indirizzo e-mail	posta
Numero di telefono	numero di telefono
Ruolo	titolo
Paese	co
Stato	stato
Dipartimento	numerodipartimento
Foto	foto
ManagerDN	manager
Gruppi	membroDi

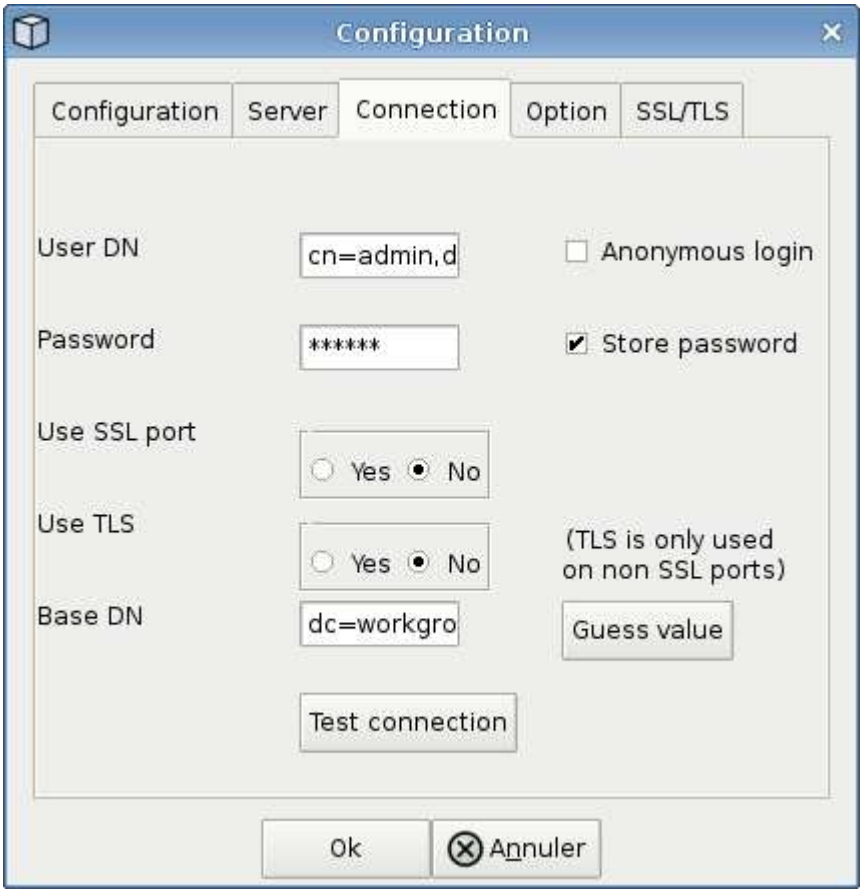
Test della configurazione del raccoglitore di directory utente

È possibile convalidare le autorizzazioni utente e le definizioni degli attributi LDAP utilizzando le seguenti procedure:

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP di Workload Security:

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Utilizzare LDAP Explorer per navigare in un database LDAP,
visualizzare le proprietà e gli attributi degli oggetti, visualizzare le
autorizzazioni, visualizzare lo schema di un oggetto, eseguire ricerche
sofisticate che è possibile salvare e rieseguire.
```

- Installa LDAP Explorer(http://ldaptool.sourceforge.net/) o Java LDAP Explorer(http://jxplorer.org/) su qualsiasi macchina Windows in grado di connettersi al server LDAP.
- Connettersi al server LDAP utilizzando il nome utente/password del server di directory LDAP.



Risoluzione dei problemi di configurazione del raccoglitore directory LDAP

Nella tabella seguente vengono descritti i problemi noti e le relative soluzioni che possono verificarsi durante la configurazione del collettore:

Problema:	Risoluzione:
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore". L'errore dice: "Credenziali non valide fornite per il server LDAP".	Bind DN o Bind Password o Search Base forniti non corretti. Modifica e fornisci le informazioni corrette.
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore". L'errore dice: "Impossibile ottenere l'oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome foresta".	Base di ricerca fornita errata. Modifica e fornisci il nome corretto della foresta.
Gli attributi facoltativi dell'utente di dominio non vengono visualizzati nella pagina Profilo utente di Workload Security.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. I campi sono sensibili alle maiuscole e alle minuscole. Modifica e fornisci i nomi corretti degli attributi facoltativi.

Problema:	Risoluzione:
Il raccoglitore dati è in stato di errore con "Impossibile recuperare gli utenti LDAP. Motivo dell'errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore cliccando sul pulsante *Riavvia*.
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore".	Assicurati di aver fornito valori validi per i campi obbligatori (Server, nome foresta, DN di associazione, password di associazione). Assicurarsi che l'input bind-DN sia sempre fornito come uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com.
L'aggiunta di un connettore di directory LDAP determina lo stato "RITIRO". Mostra l'errore "Impossibile determinare lo stato del collettore, quindi riprovare"	Assicurarsi che siano forniti l'IP del server e la base di ricerca corretti ////
Durante l'aggiunta della directory LDAP viene visualizzato il seguente errore: "Impossibile determinare lo stato del collector entro 2 tentativi, provare a riavviare nuovamente il collector (codice errore: AGENT008)"	Assicurarsi che siano forniti l'IP del server e la base di ricerca corretti
L'aggiunta di un connettore di directory LDAP determina lo stato "RITIRO". Mostra l'errore "Impossibile definire lo stato del collettore, motivo per cui il comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] non è riuscito a causa di java.net.ConnectionException:Connessione rifiutata."	IP o FQDN non corretti forniti per il server AD. Modifica e fornisci l'indirizzo IP o il nome di dominio completo (FQDN) corretto. ////
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore". L'errore dice: "Impossibile stabilire la connessione LDAP".	IP o FQDN non corretti forniti per il server LDAP. Modifica e fornisci l'indirizzo IP o il nome di dominio completo (FQDN) corretto. Oppure Valore errato per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server LDAP.
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore". L'errore dice: "Impossibile caricare le impostazioni. Motivo: la configurazione dell'origine dati presenta un errore. Motivo specifico: /connector/conf/application.conf: 70: ldap.ldap-port ha il tipo STRING anziché NUMBER"	Valore non corretto per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server AD.
Ho iniziato con gli attributi obbligatori e ha funzionato. Dopo aver aggiunto quelli facoltativi, i dati degli attributi facoltativi non vengono recuperati da AD.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. Modifica e fornisci il nome corretto dell'attributo obbligatorio o facoltativo.
Dopo aver riavviato il collector, quando avverrà la sincronizzazione LDAP?	La sincronizzazione LDAP avverrà immediatamente dopo il riavvio del collector. Ci vorranno circa 15 minuti per recuperare i dati di circa 300.000 utenti e i dati vengono aggiornati automaticamente ogni 12 ore.

Problema:	Risoluzione:
I dati utente vengono sincronizzati da LDAP a CloudSecure. Quando verranno eliminati i dati?	In caso di mancato aggiornamento, i dati dell'utente vengono conservati per 13 mesi. Se l'inquilino viene eliminato, anche i dati verranno eliminati.
Il connettore della directory LDAP genera lo stato "Errore". "Il connettore è in stato di errore. Nome del servizio: usersLdap. Motivo dell'errore: impossibile recuperare gli utenti LDAP. Motivo dell'errore: 80090308: LdapErr: DSID-0C090453, commento: errore AcceptSecurityContext, dati 52e, v3839"	Nome foresta fornito errato. Per informazioni su come fornire il nome corretto della foresta, vedere sopra.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Molto probabilmente ciò è dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare lo specifico raccoglitore di Active Directory che recupera le informazioni dell'utente da Active Directory. 2. Si noti che tra gli attributi facoltativi è presente un campo denominato "Numero di telefono" mappato all'attributo di Active Directory "telephonenumber". 4. Ora, utilizzare lo strumento Active Directory Explorer come descritto sopra per esplorare il server della directory LDAP e visualizzare il nome corretto dell'attributo. 3. Assicurarsi che nella directory LDAP sia presente un attributo denominato "numero di telefono" che contenga effettivamente il numero di telefono dell'utente. 5. Supponiamo che nella directory LDAP sia stato modificato in "numero di telefono". 6. Quindi modifica il raccoglitore CloudSecure User Directory. Nella sezione degli attributi facoltativi, sostituire 'telephonenumber' con 'phonenumber'. 7. Salvare il raccoglitore di Active Directory, il raccoglitore verrà riavviato e otterrà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è abilitato sul server Active Directory (AD), Workload Security User Directory Collector non può connettersi al server AD.	Disattivare la crittografia del server AD prima di configurare un User Directory Collector. Una volta recuperati, i dati dell'utente rimarranno disponibili per 13 mesi. Se il server AD viene disconnesso dopo aver recuperato i dettagli dell'utente, gli utenti appena aggiunti in AD non verranno recuperati. Per recuperare nuovamente la directory utente, è necessario connettersi ad AD.

Configurazione del raccoglitore dati ONTAP SVM

ONTAP SVM Data Collector consente a Workload Security di monitorare le attività di accesso ai file e agli utenti sulle macchine virtuali di storage (SVM) NetApp ONTAP . Questa guida illustra la configurazione e la gestione del raccoglitore dati SVM per garantire un monitoraggio completo della sicurezza del tuo ambiente ONTAP .

Prima di iniziare

- Questo raccoglitore di dati è supportato da quanto segue:
  - Data ONTAP 9.2 e versioni successive. Per prestazioni ottimali, utilizzare una versione Data ONTAP successiva alla 9.13.1.
  - Protocollo SMB versione 3.1 e precedenti.
  - Versioni NFS fino a NFS 4.1 inclusa (si noti che NFS 4.1 è supportato con ONTAP 9.15 o versioni successive).
  - Flexgroup è supportato da ONTAP 9.4 e versioni successive
  - FlexCache è supportato per NFS con ONTAP 9.7 e versioni successive.
  - FlexCache è supportato per SMB con ONTAP 9.14.1 e versioni successive.
  - ONTAP Select è supportato
- Sono supportati solo i tipi di dati SVM. Le SVM con volumi infiniti non sono supportate.
- SVM ha diversi sottotipi. Di questi, sono supportati solo *default*, *sync_source* e *sync_destination*.
- Un agente"deve essere configurato" prima di poter configurare i raccoglitori di dati.
- Assicurati di avere configurato correttamente un connettore directory utente, altrimenti gli eventi mostreranno nomi utente codificati e non il nome effettivo dell'utente (come memorizzato in Active Directory) nella pagina "Attività forense".
- ONTAP Persistent Store è supportato dalla versione 9.14.1.
- Per prestazioni ottimali, è consigliabile configurare il server FPolicy in modo che si trovi sulla stessa subnet del sistema di archiviazione.
- Per le migliori pratiche e raccomandazioni complete riguardanti la configurazione di Workload Security FPolicy, vedere"Articolo della Knowledge Base sulle migliori pratiche di FPolicy" .
- È necessario aggiungere una SVM utilizzando uno dei due metodi seguenti:
  - Utilizzando l'IP del cluster, il nome SVM e il nome utente e la password di gestione del cluster. ***Questo è il metodo consigliato.***
    - Il nome SVM deve essere esattamente come mostrato in ONTAP e deve essere sensibile alle maiuscole e alle minuscole.
  - Utilizzando l'IP di gestione del server virtuale SVM, nome utente e password
  - Se non si è in grado o non si desidera utilizzare il nome utente e la password completi di gestione del cluster/SVM dell'amministratore, è possibile creare un utente personalizzato con privilegi inferiori come indicato in"Una nota sui permessi" sezione sottostante. Questo utente personalizzato può essere creato per l'accesso SVM o Cluster.
    - È anche possibile utilizzare un utente AD con un ruolo che abbia almeno le autorizzazioni di csrole, come indicato nella sezione "Nota sulle autorizzazioni" di seguito. Fare riferimento anche a"Documentazione ONTAP" .
- Assicurarsi che siano impostate le applicazioni corrette per l'SVM eseguendo il seguente comando:

```
clustershell:> security login show -vserver <vservername> -user-or-group
-name <username>
```

Esempio di

output:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------  ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Assicurarsi che l'SVM abbia un server CIFS configurato: clustershell:> `vserver cifs show`

  Il sistema restituisce il nome del Vserver, il nome del server CIFS e campi aggiuntivi.

- Imposta una password per l'utente SVM vsadmin. Se si utilizza un utente personalizzato o un utente amministratore del cluster, saltare questo passaggio. clustershell:> `security login password -username vsadmin -vserver svmname`
- Sbloccare l'utente SVM vsadmin per l'accesso esterno. Se si utilizza un utente personalizzato o un utente amministratore del cluster, saltare questo passaggio. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Assicurarsi che la policy del firewall dei dati LIF sia impostata su 'mgmt' (non 'data'). Salta questo passaggio se utilizzi un lif di gestione dedicato per aggiungere l'SVM. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Quando un firewall è abilitato, è necessario definire un'eccezione per consentire il traffico TCP per la porta utilizzando Data ONTAP Data Collector.

  Vedere"Requisiti dell'agente" per informazioni sulla configurazione. Ciò vale per gli agenti on-premise e per gli agenti installati nel cloud.

- Quando un agente viene installato in un'istanza AWS EC2 per monitorare un Cloud ONTAP SVM, l'agente e lo storage devono trovarsi nella stessa VPC. Se si trovano in VPC separate, deve esserci un percorso valido tra le VPC.

Test di connettività per i collettori di dati

La funzionalità di test della connettività (introdotta a marzo 2025) ha lo scopo di aiutare gli utenti finali a identificare le cause specifiche dei guasti durante la configurazione dei raccoglitori di dati in Data Infrastructure Insights (DII) Workload Security. Ciò consente agli utenti di correggere autonomamente i problemi relativi alla comunicazione di rete o ai ruoli mancanti.

Questa funzionalità aiuterà gli utenti a determinare se tutti i controlli relativi alla rete sono stati eseguiti prima di configurare un raccoglitore dati. Inoltre, informerà gli utenti sulle funzionalità a cui possono accedere in base alla versione ONTAP , ai ruoli e alle autorizzazioni loro assegnate in ONTAP.

La connettività di prova non è supportata per i collettori di directory utente

Prerequisiti per il test di connessione

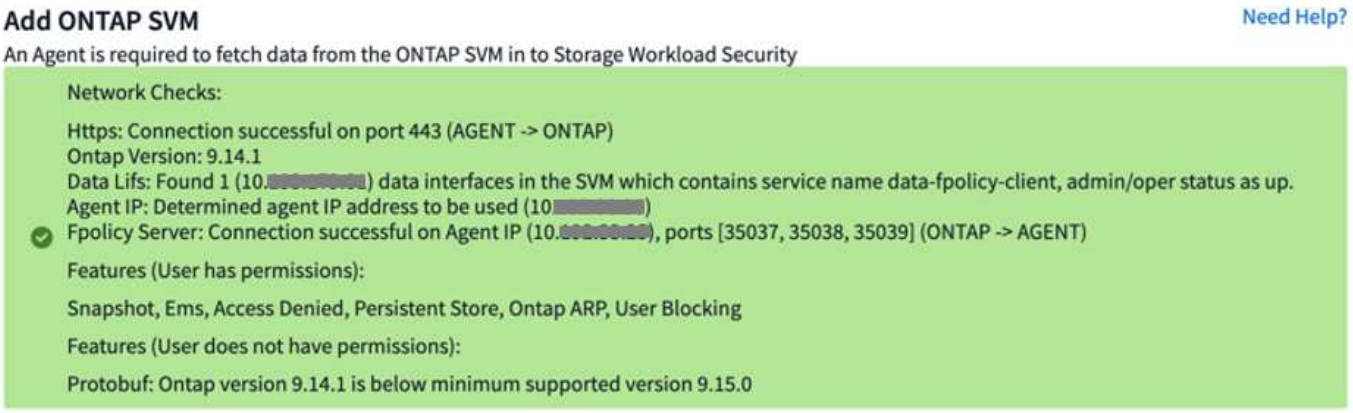
- Per il pieno funzionamento di questa funzionalità sono necessarie le credenziali a livello di cluster.
- Il controllo dell'accesso alle funzionalità non è supportato in modalità SVM.

- Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.
- Se si utilizza un utente personalizzato (ad esempio, *csuser*), fornire le autorizzazioni obbligatorie e le autorizzazioni specifiche per le funzionalità che si desidera utilizzare.

Assicurati di rivedere ilPermessi anche nella sezione sottostante.

Testare la connessione

L'utente può andare alla pagina Aggiungi/Modifica collettore, immettere i dettagli a livello di cluster (in modalità Cluster) o i dettagli a livello di SVM (in modalità SVM) e fare clic sul pulsante **Test connessione**. Workload Security elaborerà quindi la richiesta e visualizzerà un messaggio appropriato di successo o fallimento.



Cose da notare per ONTAP Multi Admin Verify (MAV)

Alcune funzionalità, come la creazione e l'eliminazione di snapshot o il blocco utente (SMB), potrebbero non funzionare in base ai comandi MAV aggiunti nella tua versione di ONTAP.

Seguire i passaggi indicati di seguito per aggiungere esclusioni ai comandi MAV che consentono a Workload Security di creare o eliminare snapshot e bloccare gli utenti.

Comandi per consentire la creazione e l'eliminazione di snapshot:

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

Comando per consentire il blocco dell'utente:

```
multi-admin-verify rule delete -operation set
```

Prerequisiti per il blocco dell'accesso utente

Tieni presente quanto segue per"Blocco dell'accesso utente" :

Per il funzionamento di questa funzionalità sono necessarie le credenziali a livello di cluster.

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni concesse all'utente, seguire i passaggi in"Blocco dell'accesso utente" per concedere a Workload Security l'autorizzazione a bloccare l'utente.

Una nota sui permessi

Autorizzazioni durante l'aggiunta tramite IP di gestione cluster:

Se non è possibile utilizzare l'utente amministratore di gestione del cluster per consentire a Workload Security di accedere al raccoglitore dati ONTAP SVM, è possibile creare un nuovo utente denominato "csuser" con i ruoli indicati nei comandi seguenti. Utilizzare il nome utente "csuser" e la password per "csuser" quando si configura il raccoglitore dati Workload Security per utilizzare l'IP di gestione cluster.

Nota: è possibile creare un singolo ruolo da utilizzare per tutte le autorizzazioni delle funzionalità per un utente personalizzato. Se esiste già un utente, eliminare prima l'utente e il ruolo esistenti utilizzando questi comandi:

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

Per creare il nuovo utente, accedere a ONTAP con il nome utente/password dell'amministratore di gestione del cluster ed eseguire i seguenti comandi sul server ONTAP :

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Autorizzazioni durante l'aggiunta tramite IP di gestione Vserver:

Se non è possibile utilizzare l'utente amministratore di gestione del cluster per consentire a Workload Security di accedere al raccoglitore dati ONTAP SVM, è possibile creare un nuovo utente denominato "csuser" con i ruoli indicati nei comandi seguenti. Utilizzare il nome utente "csuser" e la password per "csuser" quando si configura il raccoglitore dati Workload Security per utilizzare l'IP di gestione Vserver.

Nota: è possibile creare un singolo ruolo da utilizzare per tutte le autorizzazioni delle funzionalità per un utente personalizzato. Se esiste già un utente, eliminare prima l'utente e il ruolo esistenti utilizzando questi comandi:

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

Per creare il nuovo utente, accedere a ONTAP con il nome utente e la password dell'amministratore di gestione del cluster ed eseguire i seguenti comandi sul server ONTAP . Per semplicità, copia questi comandi in un editor di testo e sostituisci <vservername> con il nome del tuo Vserver prima di eseguire questi comandi su ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Modalità Protobuf

Workload Security configurerà il motore FPolicy in modalità protobuf quando questa opzione è abilitata nelle impostazioni *Configurazione avanzata* del raccoglitore. La modalità Protobuf è supportata nella versione ONTAP 9.15 e successive.

Maggiori dettagli su questa funzionalità possono essere trovati nel"Documentazione ONTAP" .

Per protobuf sono richieste autorizzazioni specifiche (alcune o tutte potrebbero già esistere):

Modalità cluster:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Modalità Vserver:
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

Autorizzazioni per la protezione autonoma da ransomware ONTAP e l'accesso negato a ONTAP

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni concesse all'utente, seguire i passaggi sottostanti per concedere a Workload Security le autorizzazioni per raccogliere informazioni relative ad ARP da ONTAP.

Per maggiori informazioni, leggi"Integrazione con ONTAP Accesso negato"

E"Integrazione con la protezione autonoma dai ransomware ONTAP"

Configurare il raccoglitore dati

Passaggi per la configurazione

1. Accedi come amministratore o proprietario dell'account al tuo ambiente Data Infrastructure Insights .
2. Fare clic su **Sicurezza del carico di lavoro > Collettori > +Collettori dati**

   Il sistema visualizza i Data Collector disponibili.

3. Passare il mouse sul riquadro * NetApp SVM e fare clic su **+Monitoraggio**.

   Il sistema visualizza la pagina di configurazione ONTAP SVM. Inserisci i dati richiesti per ogni campo.

Campo	Descrizione
Nome	Nome univoco per il Data Collector
Agente	Selezionare un agente configurato dall'elenco.
Connettiti tramite IP di gestione per:	Selezionare l'IP del cluster o l'IP di gestione SVM
Indirizzo IP di gestione cluster/SVM	L'indirizzo IP per il cluster o l'SVM, a seconda della selezione effettuata sopra.
Nome SVM	Il nome dell'SVM (questo campo è obbligatorio quando ci si connette tramite IP del cluster)
Nome utente	Nome utente per accedere a SVM/Cluster Quando si aggiunge tramite IP del cluster, le opzioni sono: 1. Cluster-admin 2. 'csuser' 3. AD-user con ruolo simile a csuser. Quando si aggiunge tramite IP SVM le opzioni sono: 4. vsadmin 5. 'csuser' 6. AD-username ha un ruolo simile a csuser.
Password	Password per il nome utente sopra indicato
Filtra Condivisioni/Volumi	Scegli se includere o escludere Condivisioni/Volumi dalla raccolta eventi
Inserisci i nomi completi delle condivisioni da escludere/includere	Elenco separato da virgole delle azioni da escludere o includere (a seconda dei casi) dalla raccolta di eventi
Inserisci i nomi completi dei volumi da escludere/includere	Elenco separato da virgole dei volumi da escludere o includere (a seconda dei casi) dalla raccolta di eventi

Monitora l’accesso alle cartelle	Se selezionata, abilita gli eventi per il monitoraggio dell’accesso alle cartelle. Si noti che la creazione/rinomina e l’eliminazione delle cartelle verranno monitorate anche senza selezionare questa opzione. Abilitando questa opzione aumenterà il numero di eventi monitorati.
Imposta la dimensione del buffer di invio ONTAP	Imposta la dimensione del buffer di invio Fpolicy ONTAP . Se si utilizza una versione ONTAP precedente alla 9.8p7 e si riscontrano problemi di prestazioni, è possibile modificare la dimensione del buffer di invio ONTAP per ottenere prestazioni ONTAP migliori. Se non vedi questa opzione e desideri provarla, contatta l’assistenza NetApp .

Dopo aver finito

- Nella pagina Collettori dati installati, utilizzare il menu delle opzioni a destra di ciascun collettore per modificare il collettore dati. È possibile riavviare il raccoglitore dati o modificarne gli attributi di configurazione.

Configurazione consigliata per MetroCluster

Per MetroCluster si consiglia quanto segue:

1. Collegare due raccoglitori di dati, uno all’SVM di origine e l’altro all’SVM di destinazione.
2. I collettori di dati devono essere connessi tramite *Cluster IP*.
3. In qualsiasi momento, il raccoglitore dati dell’SVM attualmente in esecuzione verrà visualizzato come *In esecuzione*. Il raccoglitore dati dell’SVM attualmente 'arrestato' verrà visualizzato come *Arrestato*.
4. Ogni volta che si verifica un passaggio, lo stato del raccoglitore dati cambierà da *In esecuzione* a *Arrestato* e viceversa.
5. Ci vorranno fino a due minuti affinché il raccoglitore dati passi dallo stato *Arrestato* allo stato *In esecuzione*.

Politica di servizio

Se si utilizza la policy di servizio con ONTAP **versione 9.9.1 o successiva**, per connettersi al Data Source Collector è necessario il servizio *data-fpolicy-client* insieme al servizio dati *data-nfs* e/o *data-cifs*.

Esempio:

```
Testcluster-1:*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

Nelle versioni di ONTAP precedenti alla 9.9.1, non è necessario impostare *data-fpolicy-client*.

Raccolta dati di riproduzione e pausa

Se il Data Collector è in stato *In esecuzione*, è possibile mettere in pausa la raccolta. Aprire il menu "tre punti" del raccoglitore e selezionare PAUSA. Mentre il collettore è in pausa, nessun dato viene raccolto da ONTAP e

nessun dato viene inviato dal collettore a ONTAP. Ciò significa che nessun evento Fpolicy verrà trasmesso da ONTAP al raccoglitore dati e da lì a Data Infrastructure Insights.

Si noti che se vengono creati nuovi volumi, ecc. su ONTAP mentre il raccoglitore è in pausa, Workload Security non raccoglierà i dati e tali volumi, ecc. non verranno visualizzati nei dashboard o nelle tabelle.

Un collector non può essere messo in pausa se ha utenti limitati. Ripristinare l'accesso dell'utente prima di mettere in pausa il raccoglitore.

Tieni presente quanto segue:

- L'eliminazione degli snapshot non avverrà secondo le impostazioni configurate su un collector in pausa.
- Gli eventi EMS (come ONTAP ARP) non verranno elaborati su un collector in pausa. Ciò significa che se ONTAP identifica un attacco di manomissione dei file, Data Infrastructure Insights Workload Security non sarà in grado di acquisire quell'evento.
- Le email di notifica sullo stato di salute NON verranno inviate per un raccoglitore in pausa.
- Le azioni manuali o automatiche (ad esempio Snapshot o Blocco utente) non saranno supportate su un collector in pausa.
- Durante gli aggiornamenti dell'agente o del collettore, i riavvii/riavvii della VM dell'agente o il riavvio del servizio dell'agente, un collettore in pausa rimarrà nello stato *Paused*.
- Se il raccoglitore dati è nello stato *Errore*, non è possibile modificarlo nello stato *Pausa*. Il pulsante Pausa sarà abilitato solo se lo stato del raccoglitore è *In esecuzione*.
- Se l'agente è disconnesso, non è possibile modificare lo stato del collettore in *Pausa*. Il raccoglitore passerà allo stato *Arrestato* e il pulsante Pausa verrà disabilitato.

Archivio persistente

L'archivio persistente è supportato con ONTAP 9.14.1 e versioni successive. Si noti che le istruzioni relative al nome del volume variano da ONTAP 9.14 a 9.15.

È possibile abilitare Persistent Store selezionando la casella di controllo nella pagina di modifica/aggiunta del raccoglitore. Dopo aver selezionato la casella di controllo, viene visualizzato un campo di testo per accettare il nome del volume. Il nome del volume è un campo obbligatorio per abilitare Persistent Store.

- Per ONTAP 9.14.1, è necessario creare il volume prima di abilitare la funzionalità e fornire lo stesso nome nel campo *Nome volume*. La dimensione consigliata del volume è 16 GB.
- Per ONTAP 9.15.1, il volume verrà creato automaticamente con una dimensione di 16 GB dal collettore, utilizzando il nome fornito nel campo *Nome volume*.

Per Persistent Store sono necessarie autorizzazioni specifiche (alcune o tutte potrebbero già esistere):

Modalità cluster:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Modalità Vserver:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

Migrazione dei collezionisti

È possibile migrare facilmente un collettore Workload Security da un agente all'altro, consentendo un efficiente bilanciamento del carico dei collettori tra gli agenti.

Prerequisiti

- L'agente sorgente deve essere nello stato *connesso*.
- Il collector da migrare deve essere nello stato *running*.

Nota:

- La migrazione è supportata sia per i raccoglitori di dati che per quelli di directory utente.
- La migrazione di un collector non è supportata per i tenant gestiti manualmente.

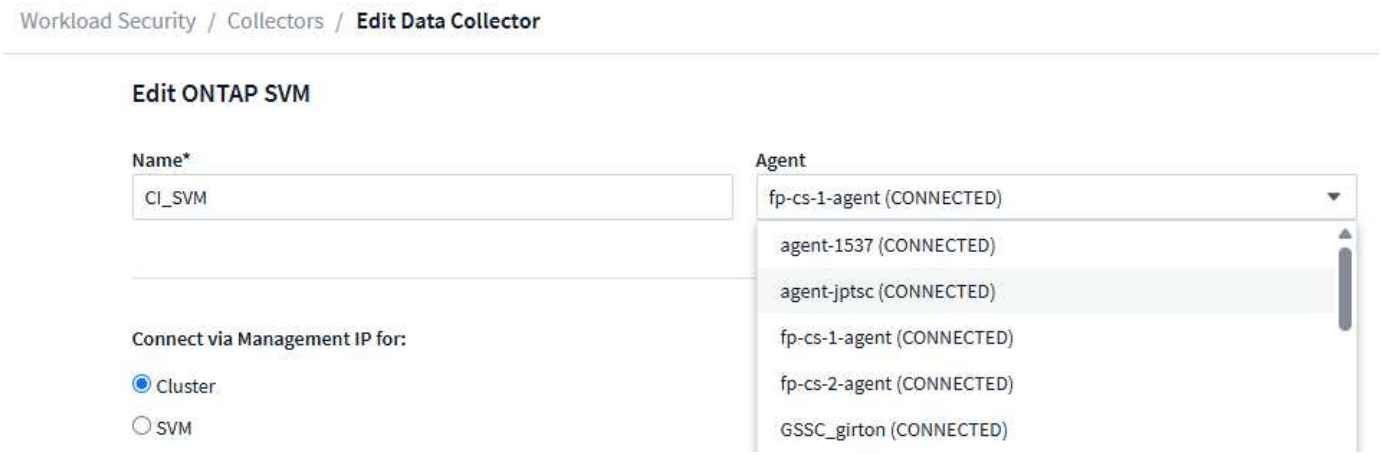
Migrare il raccoglitore

Per migrare un collector, seguire questi passaggi:

1. Vai alla pagina "Modifica raccoglitore".
2. Selezionare un agente di destinazione dal menu a discesa degli agenti.
3. Fare clic sul pulsante "Salva raccoglitore".

Workload Security elaborerà la richiesta. Una volta completata la migrazione, l'utente verrà reindirizzato alla pagina dell'elenco dei collezionisti. In caso di errore, verrà visualizzato un messaggio appropriato nella pagina di modifica.

Nota: tutte le modifiche alla configurazione apportate in precedenza nella pagina "Modifica raccoglitore" rimarranno applicate quando il raccoglitore verrà migrato correttamente all'agente di destinazione.



Risoluzione dei problemi

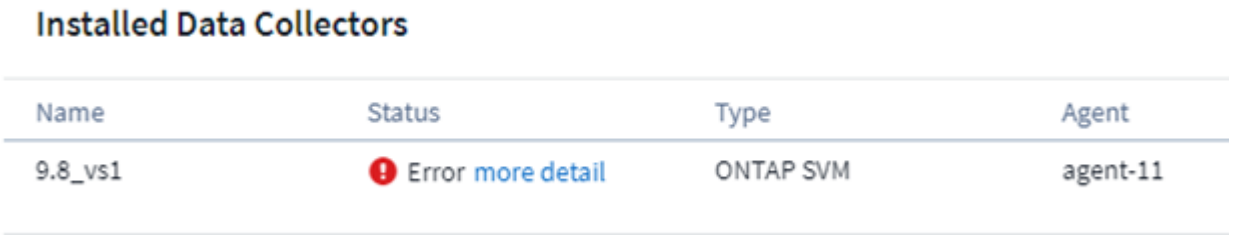
Vedi il"Risoluzione dei problemi del collettore SVM" pagina per suggerimenti sulla risoluzione dei problemi.

Risoluzione dei problemi del raccoglitore dati ONTAP SVM

Workload Security utilizza dei collettori di dati per raccogliere dati sui file e sugli accessi degli utenti dai dispositivi. Qui puoi trovare suggerimenti per la risoluzione dei problemi relativi a questo raccoglitore.

Vedi il"Configurazione del collettore SVM" pagina per le istruzioni sulla configurazione di questo raccoglitore.

In caso di errore, è possibile fare clic su *ulteriori dettagli* nella colonna *Stato* della pagina Collettori dati installati per ottenere maggiori dettagli sull'errore.



Di seguito vengono descritti i problemi noti e le relative soluzioni.

Problema: Data Collector funziona per un po' di tempo e si arresta dopo un tempo casuale, con il seguente messaggio di errore: "Messaggio di errore: il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno sovraccarico." **Prova questo:** la frequenza degli eventi di ONTAP era molto più alta di quella che la casella Agent può gestire. Di conseguenza la connessione è stata interrotta.

Controlla il picco di traffico in CloudSecure al momento della disconnessione. Puoi verificarlo dalla pagina **CloudSecure > Activity Forensics > Tutte le attività**.

Se il traffico aggregato di picco è superiore a quello che l'Agent Box può gestire, fare riferimento alla pagina Event Rate Checker per informazioni su come dimensionare la distribuzione del Collector in un Agent Box.

Se l'agente è stato installato nella casella Agente prima del 4 marzo 2021, eseguire i seguenti comandi nella casella Agente:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Dopo il ridimensionamento, riavviare il raccoglitore dall'interfaccia utente.

{vuoto}

Problema: il Collector segnala il messaggio di errore: "Nessun indirizzo IP locale trovato sul connettore in

grado di raggiungere le interfacce dati dell'SVM". **Prova questo:** Molto probabilmente è dovuto a un problema di rete sul lato ONTAP . Si prega di seguire questi passaggi:

1. Assicurarsi che non vi siano firewall sulla vita dati SVM o sulla vita di gestione che bloccano la connessione dalla SVM.
2. Quando si aggiunge una SVM tramite un IP di gestione del cluster, assicurarsi che la vita dati e la vita di gestione della SVM siano pingabili dalla VM dell'agente. In caso di problemi, controllare il gateway, la netmask e i percorsi per lif.

   Puoi anche provare ad accedere al cluster tramite ssh utilizzando l'IP di gestione del cluster ed effettuare il ping dell'IP dell'agente. Assicurarsi che l'IP dell'agente sia pingabile:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

3. Se hai provato a connetterti tramite l'IP del cluster e non funziona, prova a connetterti direttamente tramite l'IP SVM. Per i passaggi necessari per connettersi tramite IP SVM, vedere quanto sopra.
4. Durante l'aggiunta del collettore tramite IP SVM e credenziali vsadmin, verificare se SVM Lif ha abilitato il ruolo Data plus Mgmt. In questo caso il ping all'SVM Lif funzionerà, ma l'SSH all'SVM Lif non funzionerà. In caso affermativo, creare un SVM Mgmt Only Lif e provare a connettersi tramite questo SVM Management Only Lif.
5. Se ancora non funziona, crea un nuovo SVM Lif e prova a connetterti tramite quel Lif. Assicurarsi che la subnet mask sia impostata correttamente.
6. Debug avanzato:
   a. Avvia una traccia dei pacchetti in ONTAP.
   b. Provare a connettere un data collector all'SVM dall'interfaccia utente di CloudSecure.
   c. Attendi finché non compare l'errore. Arresta la traccia dei pacchetti in ONTAP.
   d. Aprire la traccia del pacchetto da ONTAP. È disponibile in questa posizione

      ```
       https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
      .. Assicurarsi che ci sia un SYN da ONTAP alla casella Agent.
      .. Se non c'è SYN da ONTAP , allora c'è un problema con il firewall
      in ONTAP.
      .. Aprire il firewall in ONTAP, in modo che ONTAP possa connettersi
      alla casella agente.
      ```

7. Se il problema persiste, consultare il team di rete per accertarsi che nessun firewall esterno stia bloccando la connessione da ONTAP alla casella Agent.
8. Se nessuna delle soluzioni precedenti risolve il problema, apri un caso con"Supporto Netapp" per ulteriore assistenza.

{vuoto}

Problema: Messaggio: "Impossibile determinare il tipo ONTAP per [nome host: <indirizzo IP>. Motivo: Errore di connessione al sistema di archiviazione <Indirizzo IP>: Host non raggiungibile (Host non raggiungibile)
Prova questo:

1. Verificare che sia stato fornito l'indirizzo IP di gestione SVM o l'IP di gestione del cluster corretto.
2. Eseguire l'SSH sull'SVM o sul Cluster a cui si intende connettersi. Una volta effettuata la connessione, assicurarsi che il nome SVM o Cluster sia corretto.

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno terminato." **Prova questo:**

1. È molto probabile che un firewall stia bloccando le porte necessarie nella macchina dell'agente. Verificare che l'intervallo di porte 35000-55000/tcp sia aperto affinché la macchina agente possa connettersi dall'SVM. Assicurarsi inoltre che non vi siano firewall abilitati sul lato ONTAP che bloccano la comunicazione con la macchina agente.
2. Digitare il seguente comando nella casella Agente e assicurarsi che l'intervallo di porte sia aperto.

   ```
   sudo iptables-save | grep 3500*
   ```

   L'output di esempio dovrebbe apparire così:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Accedi a SVM, inserisci i seguenti comandi e verifica che non sia
   impostato alcun firewall per bloccare la comunicazione con ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Controlla i comandi del firewall"sul lato ONTAP .

3. Accedi tramite SSH all'SVM/Cluster che vuoi monitorare. Eseguire il ping della casella Agent dalla libreria dati SVM (con supporto dei protocolli CIFS e NFS) e assicurarsi che il ping funzioni:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

4. Se un singolo SVM viene aggiunto due volte a un tenant tramite 2 collettori dati, verrà visualizzato questo errore. Eliminare uno dei collettori di dati tramite l'interfaccia utente. Quindi riavviare l'altro raccoglitore dati

tramite l'interfaccia utente. Quindi il raccoglitore dati mostrerà lo stato "IN ESECUZIONE" e inizierà a ricevere eventi da SVM.

In pratica, in un tenant, 1 SVM dovrebbe essere aggiunto una sola volta, tramite 1 data collector. 1 SVM non dovrebbe essere aggiunto due volte tramite 2 collettori di dati.

5. Nei casi in cui lo stesso SVM è stato aggiunto in due diversi ambienti Workload Security (tenant), l'ultimo riuscirà sempre. Il secondo collettore configurerà fpolicy con il proprio indirizzo IP ed espellerà il primo. Quindi il collettore nel primo smetterà di ricevere eventi e il suo servizio di "audit" entrerà in stato di errore. Per evitare ciò, configurare ogni SVM su un singolo ambiente.
6. Questo errore può verificarsi anche se i criteri di servizio non sono configurati correttamente. Con ONTAP 9.8 o versioni successive, per connettersi al Data Source Collector, è necessario il servizio data-fpolicy-client insieme al servizio dati data-nfs e/o data-cifs. Inoltre, il servizio data-fpolicy-client deve essere associato ai dati lif per l'SVM monitorato.

{vuoto}

Problema: Nessun evento visualizzato nella pagina delle attività. **Prova questo:**

1. Verificare se il collettore ONTAP è nello stato "IN ESECUZIONE". In caso affermativo, assicurarsi che alcuni eventi cifs vengano generati sulle VM client cifs aprendo alcuni file.
2. Se non vengono rilevate attività, effettuare l'accesso all'SVM e immettere il seguente comando.

```
<SVM>event log show -source fpolicy
```

   Assicurati che non ci siano errori relativi a fpolicy.

3. Se non vengono visualizzate attività, effettuare l'accesso all'SVM. Immettere il seguente comando:

```
<SVM>fpolicy show
```

   Verificare se la policy fpolicy denominata con prefisso "cloudsecure_" è stata impostata e lo stato è "on". Se non è impostato, molto probabilmente l'agente non è in grado di eseguire i comandi nell'SVM. Si prega di assicurarsi che siano stati rispettati tutti i prerequisiti descritti all'inizio della pagina.

{vuoto}

Problema: SVM Data Collector è in stato di errore e il messaggio di errore è "L'agente non è riuscito a connettersi al raccoglitore". **Prova questo:**

1. Molto probabilmente l'agente è sovraccarico e non riesce a connettersi ai collettori dell'origine dati.
2. Controllare quanti collettori di origini dati sono connessi all'agente.
3. Controllare anche la velocità del flusso di dati nella pagina "Tutte le attività" nell'interfaccia utente.
4. Se il numero di attività al secondo è significativamente elevato, installare un altro agente e spostare alcuni dei Data Source Collector sul nuovo agente.

{vuoto}

Problema: SVM Data Collector mostra il messaggio di errore "fpolicy.server.connectError: il nodo non è riuscito a stabilire una connessione con il server FPolicy "12.195.15.146" (motivo: "Selezione scaduta")" **Prova questo:** il firewall è abilitato in SVM/Cluster. Quindi il motore fpolicy non è in grado di connettersi al server fpolicy. Le CLI in ONTAP che possono essere utilizzate per ottenere maggiori informazioni sono:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Controlla i comandi del firewall"sul lato ONTAP .

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Nessuna interfaccia dati valida (ruolo: dati, protocolli dati: NFS o CIFS o entrambi, stato: attivo) trovata sull'SVM." **Prova questo:** assicurati che ci sia un'interfaccia operativa (che abbia il ruolo di dati e protocollo dati come CIFS/NFS).

{vuoto}

Problema: il raccoglitore dati entra nello stato di errore e poi, dopo un po' di tempo, passa allo stato di esecuzione, per poi tornare nuovamente allo stato di errore. Questo ciclo si ripete. **Prova questo:** Questo accade in genere nel seguente scenario:

1. Sono stati aggiunti più raccoglitori di dati.
2. Ai collettori di dati che mostrano questo tipo di comportamento verrà aggiunto 1 SVM. Ciò significa che 2 o più collettori di dati sono collegati a 1 SVM.
3. Assicurarsi che 1 raccoglitore dati si connetta a 1 solo SVM.
4. Eliminare gli altri raccoglitori di dati connessi allo stesso SVM.

{vuoto}

Problema: Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare (policy su SVM svmname. Motivo: Valore non valido specificato per l'elemento 'shares-to-include' in 'fpolicy.policy.scope-modify: "Federal' **Prova questo:** *I nomi delle condivisioni devono essere specificati senza virgolette. Modificare la configurazione DSC ONTAP SVM per correggere i nomi delle condivisioni.

Includi ed escludi azioni non è pensato per un lungo elenco di nomi di azioni. Se hai un gran numero di azioni da includere o escludere, utilizza il filtro per volume.

{vuoto}

Problema: Nel cluster sono presenti fpolicies esistenti che non sono utilizzati. Cosa si dovrebbe fare prima di installare Workload Security? **Prova questo:** Si consiglia di eliminare tutte le impostazioni fpolicy esistenti e non utilizzate, anche se sono in stato disconnesso. Workload Security creerà fpolicy con il prefisso "cloudsecure_". Tutte le altre configurazioni fpolicy non utilizzate possono essere eliminate.

Comando CLI per visualizzare l'elenco fpolicy:

```
 fpolicy show
Passaggi per eliminare le configurazioni fpolicy:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vuoto}

Problema: Dopo aver abilitato Workload Security, le prestazioni ONTAP risultano compromesse: la latenza diventa sporadicamente elevata, mentre gli IOPS diventano sporadicamente bassi. **Prova questo:** Durante l'utilizzo di ONTAP con Workload Security, a volte si possono verificare problemi di latenza in ONTAP. Le possibili cause di ciò sono molteplici, come indicato di seguito:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tutti questi problemi sono stati risolti in ONTAP 9.13.1 e versioni successive; si consiglia vivamente di utilizzare una di queste versioni successive.

{vuoto}

Problema: Data Collector mostra il messaggio di errore: "Errore: impossibile determinare lo stato del collector entro 2 tentativi, provare a riavviare nuovamente il collector (codice errore: AGENT008)". **Prova questo:**

1. Nella pagina dei raccoglitori di dati, scorrere verso destra del raccoglitore di dati che ha generato l'errore e fare clic sul menu con i 3 puntini. Selezionare *Modifica*. Inserire nuovamente la password del raccoglitore dati. Salvare il raccoglitore dati premendo il pulsante *Salva*. Data Collector verrà riavviato e l'errore dovrebbe essere risolto.
2. La macchina dell'agente potrebbe non avere abbastanza CPU o RAM, ecco perché i DSC non funzionano. Controllare il numero di Data Collector aggiunti all'agente nella macchina. Se è superiore a 20, aumentare la capacità della CPU e della RAM della macchina agente. Una volta aumentata la CPU e la RAM, i DSC entreranno automaticamente nello stato di inizializzazione e poi in quello di esecuzione. Consulta la guida alle taglie su"questa pagina" .

{vuoto}

Problema: il Data Collector genera un errore quando è selezionata la modalità SVM. **Prova questo:** durante

la connessione in modalità SVM, se per la connessione viene utilizzato l'IP di gestione del cluster anziché l'IP di gestione SVM, la connessione genererà un errore. Assicurarsi che venga utilizzato l'IP SVM corretto.

{vuoto}

Problema: Il raccoglitore dati mostra un messaggio di errore quando la funzione Accesso negato è abilitata: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: impossibile configurare fpolicy su SVM test_svm. Motivo: L'utente non è autorizzato." **Prova questo:** L'utente potrebbe non disporre delle autorizzazioni REST necessarie per la funzionalità Accesso negato. Si prega di seguire le istruzioni su"questa pagina" per impostare i permessi.

Una volta impostate le autorizzazioni, riavviare il raccoglitore.

{vuoto}

Problema: Il collettore è in stato di errore con il messaggio: Il connettore è in stato di errore. Motivo dell'errore: impossibile configurare l'archivio persistente su SVM <Nome SVM>. Motivo: impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova il comando. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare l'archivio persistente su SVM <SVM Name>. Motivo: Impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova a eseguire il comando.

Prova questo: attendi qualche minuto e poi riavvia il Collector.

{vuoto}

Se riscontri ancora problemi, contatta l'assistenza tramite i link indicati nella pagina **Aiuto > Assistenza**.

Configurazione di Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP

Monitora l'accesso ai file e agli utenti nell'intera infrastruttura di archiviazione cloud configurando i raccoglitori di dati Workload Security per Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP. Questa guida fornisce istruzioni dettagliate per distribuire gli agenti in AWS e connetterli alle istanze di archiviazione cloud.

Configurazione di archiviazione Cloud Volumes ONTAP

Consultare la documentazione di OnCommand Cloud Volumes ONTAP per configurare un'istanza AWS a nodo singolo/HA per ospitare Workload Security Agent:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Una volta completata la configurazione, segui i passaggi per impostare la tua SVM:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Piattaforme supportate

- Cloud Volumes ONTAP, supportato da tutti i provider di servizi cloud disponibili, ove disponibili. Ad esempio: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Configurazione della macchina agente

La macchina agente deve essere configurata nelle rispettive subnet dei provider di servizi cloud. Per ulteriori informazioni sull'accesso alla rete, consultare [Requisiti dell'agente].

Di seguito sono riportati i passaggi per l'installazione dell'agente in AWS. Per l'installazione, è possibile seguire passaggi equivalenti, a seconda del provider di servizi cloud, in Azure o Google Cloud.

In AWS, attenersi alla seguente procedura per configurare la macchina da utilizzare come agente di sicurezza del carico di lavoro:

Per configurare la macchina da utilizzare come Workload Security Agent, attenersi alla seguente procedura:

Passi

1. Accedi alla console AWS, vai alla pagina EC2-Instances e seleziona *Avvia istanza*.
2. Selezionare un'AMI RHEL o CentOS con la versione appropriata come indicato in questa pagina:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Selezionare la VPC e la subnet in cui risiede l'istanza Cloud ONTAP .
4. Selezionare *t2.xlarge* (4 vCPU e 16 GB di RAM) come risorse allocate.
    a. Creare l'istanza EC2.
5. Installare i pacchetti Linux richiesti utilizzando il gestore pacchetti YUM:
    a. Installa i pacchetti Linux nativi *wget* e *unzip*.

Installare l'agente di sicurezza del carico di lavoro

1. Accedi come amministratore o proprietario dell'account al tuo ambiente Data Infrastructure Insights .
2. Passare a **Collectors** di Workload Security e fare clic sulla scheda **Agents**.
3. Fare clic su **+Agente** e specificare RHEL come piattaforma di destinazione.
4. Copiare il comando Installazione agente.
5. Incolla il comando Agent Installation nell'istanza RHEL EC2 a cui hai effettuato l'accesso. Questo installa l'agente Workload Security, fornendo tutti i"Prerequisiti dell'agente" sono soddisfatte.

Per i passaggi dettagliati, fare riferimento a questo collegamento: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Risoluzione dei problemi

Nella tabella seguente sono descritti i problemi noti e le relative soluzioni.

Problema	Risoluzione

Il Data Collector mostra l'errore "Sicurezza del carico di lavoro: impossibile determinare il tipo di ONTAP per il raccoglitore dati Amazon FxSN". Il cliente non è in grado di aggiungere un nuovo raccoglitore dati Amazon FSxN in Workload Security. La connessione al cluster FSxN sulla porta 443 dall'agente è in timeout. Il firewall e i gruppi di sicurezza AWS hanno le regole necessarie abilitate per consentire la comunicazione. Un agente è già distribuito e si trova anche nello stesso account AWS. Questo stesso agente viene utilizzato per connettere e monitorare i restanti dispositivi NetApp (e tutti funzionano).	Risolvi questo problema aggiungendo il segmento di rete LIF di fsxadmin alla regola di sicurezza dell'agente. Se non sei sicuro delle porte, consenti tutte le porte.

Gestione degli utenti

Gli account utente di Workload Security vengono gestiti tramite Data Infrastructure Insights.

Data Infrastructure Insights fornisce quattro livelli di account utente: proprietario dell'account, amministratore, utente e ospite. A ciascun account vengono assegnati livelli di autorizzazione specifici. Un account utente con privilegi di amministratore può creare o modificare utenti e assegnare a ciascun utente uno dei seguenti ruoli di sicurezza del carico di lavoro:

Ruolo	Accesso alla sicurezza del carico di lavoro
Amministratore	Può eseguire tutte le funzioni di sicurezza del carico di lavoro, comprese quelle per avvisi, analisi forense, raccoglitori di dati, criteri di risposta automatizzati e API per la sicurezza del carico di lavoro. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di sicurezza del carico di lavoro.
Utente	Può visualizzare e gestire gli avvisi e visualizzare le analisi forensi. Il ruolo utente può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot e limitare l'accesso utente.
Ospite	È possibile visualizzare avvisi e analisi forensi. Il ruolo ospite non può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot o limitare l'accesso degli utenti.

Passi

1. Accedi a Workload Security
2. Nel menu, fare clic su **Amministrazione > Gestione utenti**

   Verrai indirizzato alla pagina Gestione utenti di Data Infrastructure Insights.

3. Selezionare il ruolo desiderato per ciascun utente.

Quando si aggiunge un nuovo utente, è sufficiente selezionare il ruolo desiderato (solitamente Utente o Ospite).

Ulteriori informazioni sugli account utente e sui ruoli sono disponibili in Data Infrastructure Insights"Ruolo utente" documentazione.

Event Rate Checker: Guida alle dimensioni degli agenti

Determina il dimensionamento ottimale delle macchine Agent misurando le frequenze degli eventi NFS e SMB generate dalle tue SVM prima di distribuire i data collector. Lo script Event Rate Checker ti aiuta a comprendere i limiti di capacità (massimo 50 data collector per Agent) e garantisce che la tua infrastruttura Agent possa gestire il volume di eventi previsto per un rilevamento affidabile delle minacce.

Requisiti:

- IP del cluster
- Nome utente e password dell'amministratore del cluster

Quando si esegue questo script, non deve essere in esecuzione alcun ONTAP SVM Data Collector per l'SVM per cui si sta determinando la frequenza degli eventi.

Passaggi:

1. Installare l'agente seguendo le istruzioni in CloudSecure.
2. Una volta installato l'agente, eseguire lo script *server_data_rate_checker.sh* come utente sudo:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Questo script richiede che _sshpass_ sia installato sulla macchina
Linux.  Ci sono due modi per installarlo:
```

   a. Esegui il seguente comando:

```
 linux_prompt> yum install sshpass
.. Se ciò non funziona, scarica _sshpass_ dal web sul computer Linux
ed esegui il seguente comando:
```

```
linux_prompt> rpm -i sshpass
```

3. Fornire i valori corretti quando richiesto. Di seguito è riportato un esempio.
4. L'esecuzione dello script richiederà circa 5 minuti.
5. Una volta completata l'esecuzione, lo script stamperà la frequenza degli eventi dall'SVM. È possibile controllare la frequenza degli eventi per SVM nell'output della console:

```
"Svm svm_rate is generating 100 events/sec".
```

Ogni Ontap SVM Data Collector può essere associato a un singolo SVM, il che significa che ogni data collector sarà in grado di ricevere il numero di eventi generati da un singolo SVM.

Tieni presente quanto segue:

A) Utilizzare questa tabella come guida generale alle taglie. È possibile aumentare il numero di core e/o di memoria per aumentare il numero di collettori dati supportati, fino a un massimo di 50 collettori dati:

Configurazione della macchina agente	Numero di collettori di dati SVM	Frequenza massima degli eventi che la macchina agente può gestire
4 core, 16 GB	10 raccoglitori di dati	20K eventi/sec
4 core, 32 GB	20 raccoglitori di dati	20K eventi/sec

B) Per calcolare il totale degli eventi, sommare gli eventi generati per tutti gli SVM per quell'agente.

C) Se lo script non viene eseguito durante le ore di punta o se è difficile prevedere il traffico di punta, mantenere un buffer di frequenza degli eventi del 30%.

B + C Dovrebbe essere minore di A, altrimenti la macchina agente non riuscirà a monitorare.

In altre parole, il numero di collettori di dati che possono essere aggiunti a una singola macchina agente dovrebbe essere conforme alla formula seguente:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Vedi illink:concept_cs_agent_requirements.html["Requisiti dell'agente"]
pagina per ulteriori prerequisiti e requisiti.
```

Esempio

Supponiamo di avere tre SVMS che generano frequenze di eventi rispettivamente di 100, 200 e 300 eventi al secondo.

Applichiamo la formula:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

L'output della console è disponibile nella macchina dell'agente nel nome file *fpolicy_stat_<Nome SVM>.log* nella directory di lavoro corrente.

Lo script potrebbe dare risultati errati nei seguenti casi:

- Sono state fornite credenziali, IP o nome SVM errati.
- Una fpolicy già esistente con lo stesso nome, numero di sequenza, ecc. genererà un errore.
- Lo script si interrompe bruscamente durante l'esecuzione.

Di seguito è riportato un esempio di esecuzione dello script:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

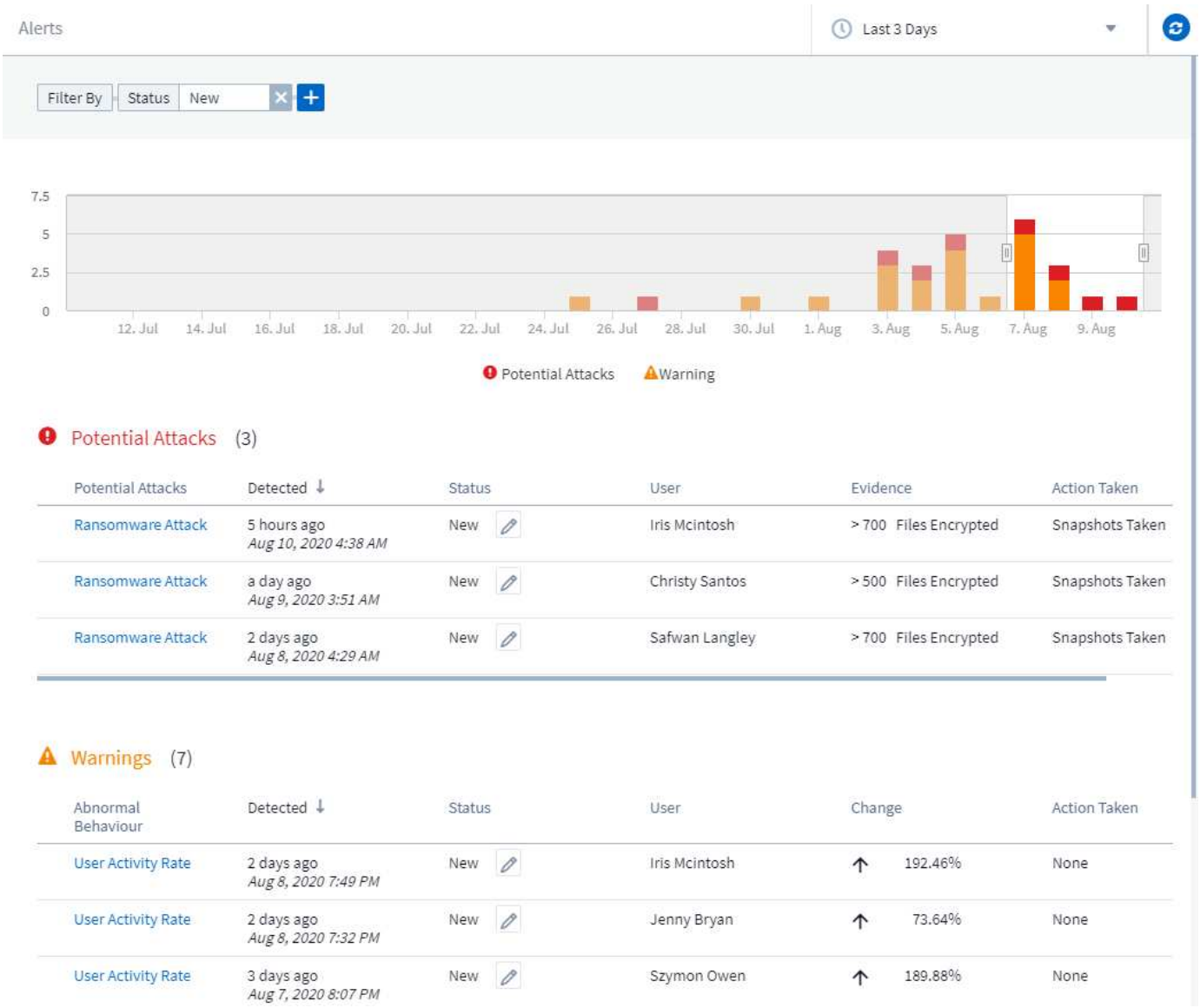
```
[root@ci-cs-data agent]#
```

Risoluzione dei problemi

Domanda	Risposta
Se eseguo questo script su una SVM già configurata per Workload Security, utilizza semplicemente la configurazione fpolicy esistente sulla SVM oppure ne imposta una temporanea ed esegue il processo?	Event Rate Checker può funzionare correttamente anche per una SVM già configurata per Workload Security. Non dovrebbe esserci alcun impatto.
Posso aumentare il numero di SVM su cui può essere eseguito lo script?	Sì. Basta modificare lo script e cambiare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se aumento il numero di SVM, aumenterà il tempo di esecuzione dello script?	No. Lo script verrà eseguito per un massimo di 5 minuti, anche se il numero di SVM viene aumentato.
Posso aumentare il numero di SVM su cui può essere eseguito lo script?	Sì. È necessario modificare lo script e cambiare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se aumento il numero di SVM, aumenterà il tempo di esecuzione dello script?	No. Lo script verrà eseguito per un massimo di 5 minuti, anche se il numero di SVM viene aumentato.
Cosa succede se eseguo Event Rate Checker con un agente esistente?	L'esecuzione di Event Rate Checker su un agente già esistente potrebbe causare un aumento della latenza sull'SVM. Questo aumento sarà di natura temporanea mentre è in esecuzione Event Rate Checker.

Comprendere e indagare gli avvisi

La pagina Avvisi sulla sicurezza del carico di lavoro fornisce una cronologia completa delle minacce e degli avvisi rilevati, con strumenti di indagine dettagliati. Visualizza i dettagli degli avvisi, gestisci gli aggiornamenti di stato, filtra in base a criteri e monitora le attività degli utenti per indagare e rispondere in modo efficiente agli incidenti di sicurezza.



Attenzione

L'elenco degli avvisi visualizza un grafico che mostra il numero totale di potenziali attacchi e/o avvisi emessi nell'intervallo di tempo selezionato, seguito da un elenco degli attacchi e/o avvisi verificatisi in tale intervallo di tempo. È possibile modificare l'intervallo di tempo regolando i cursori dell'ora di inizio e dell'ora di fine nel grafico.

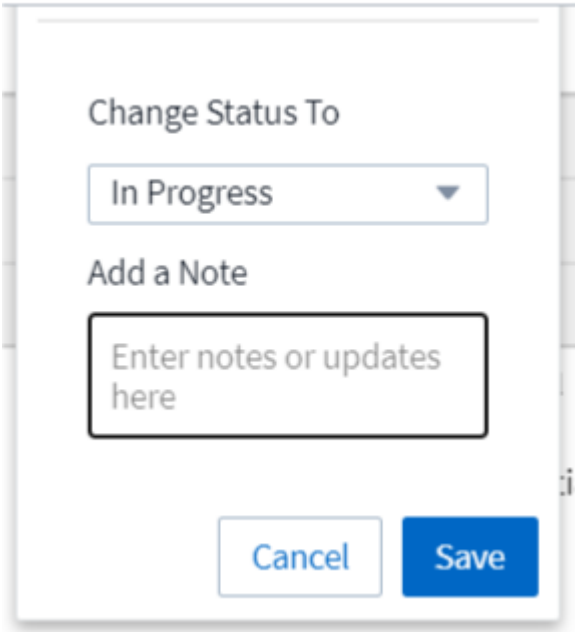
Per ogni avviso viene visualizzato quanto segue:

Potenziali attacchi:

- Il tipo di *Potenziale attacco* (ad esempio, manomissione di file o sabotaggio)
- Data e ora in cui è stato rilevato il potenziale attacco
- Lo *Stato* dell'avviso:
  - **Nuovo**: questa è l'impostazione predefinita per i nuovi avvisi.
  - **In corso**: l'avviso è in fase di analisi da parte di uno o più membri del team.
  - **Risolto**: l'avviso è stato contrassegnato come risolto da un membro del team.

- **Ignorato**: l'avviso è stato ignorato come falso positivo o comportamento previsto.

  Un amministratore può modificare lo stato dell'avviso e aggiungere una nota per facilitare l'indagine.



- L'*Utente* il cui comportamento ha attivato l'avviso
- *Prova* dell'attacco (ad esempio, un gran numero di file è stato crittografato)
- L'*azione intrapresa* (ad esempio, è stata scattata un'istantanea)

Avvertenze:

- Il *comportamento anomalo* che ha attivato l'avviso
- La data e l'ora in cui il comportamento è stato *Rilevato*
- Lo *Stato* dell'avviso (Nuovo, In corso, ecc.)
- L'*Utente* il cui comportamento ha attivato l'avviso
- Una descrizione della *Modifica* (ad esempio, un aumento anomalo dell'accesso ai file)
- L'azione intrapresa

Opzioni filtro

Puoi filtrare gli avvisi in base a quanto segue:

- Lo *Stato* dell'avviso
- Testo specifico nella *Nota*
- Il tipo di *Attacchi/Avvisi*
- L'*Utente* le cui azioni hanno attivato l'avviso/segnalazione

La pagina Dettagli avviso

È possibile fare clic sul collegamento di un avviso nella pagina dell'elenco degli avvisi per aprire una pagina dei dettagli dell'avviso. I dettagli dell'avviso possono variare a seconda del tipo di attacco o di avviso. Ad

esempio, una pagina con i dettagli di un attacco di manomissione di file potrebbe mostrare le seguenti informazioni:

Sezione riassuntiva:

- Tipo di attacco (manomissione di file, sabotaggio) e ID avviso (assegnato da Workload Security)
- Data e ora in cui è stato rilevato l'attacco
- Azione intrapresa (ad esempio, è stata scattata un'istantanea automatica). L'ora dello snapshot è mostrata immediatamente sotto la sezione di riepilogo))
- Stato (Nuovo, In corso, ecc.)

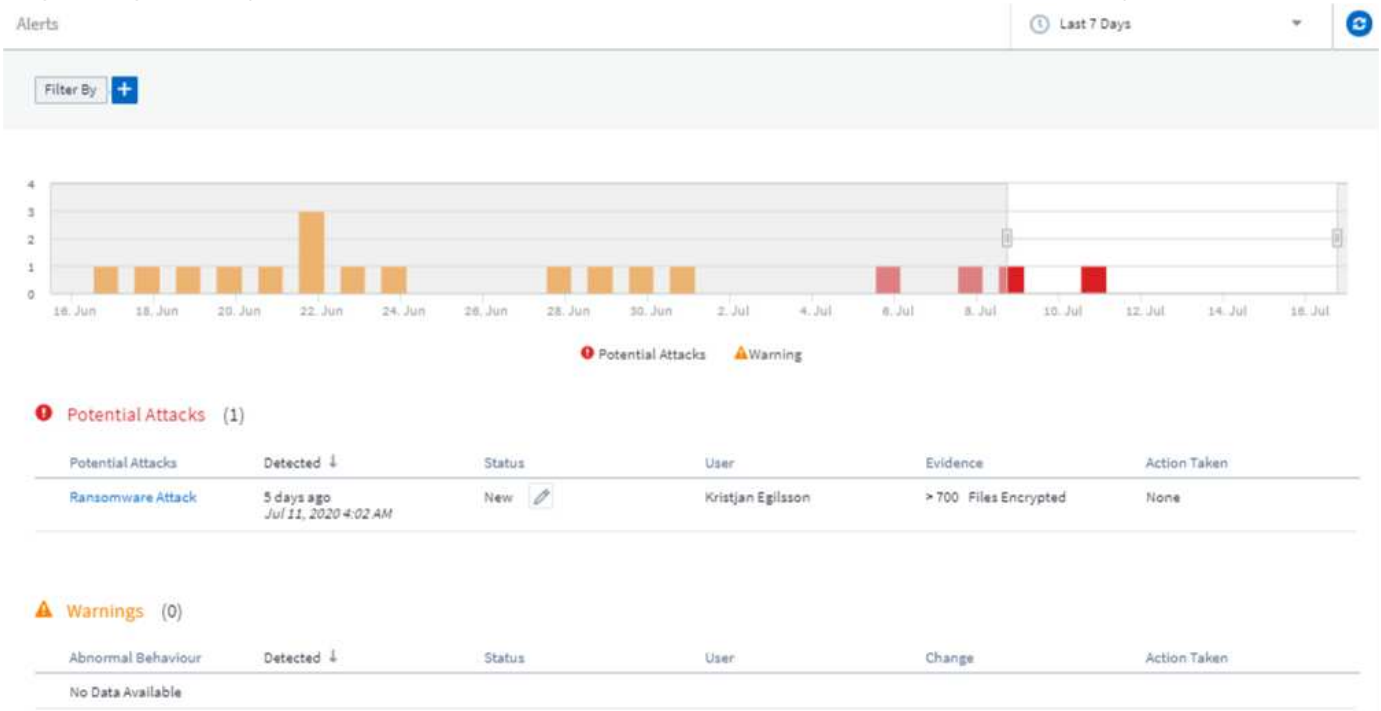
Sezione Risultati dell'attacco:

- Conteggio dei volumi e dei file interessati
- Un riassunto allegato del rilevamento
- Un grafico che mostra l'attività del file durante l'attacco

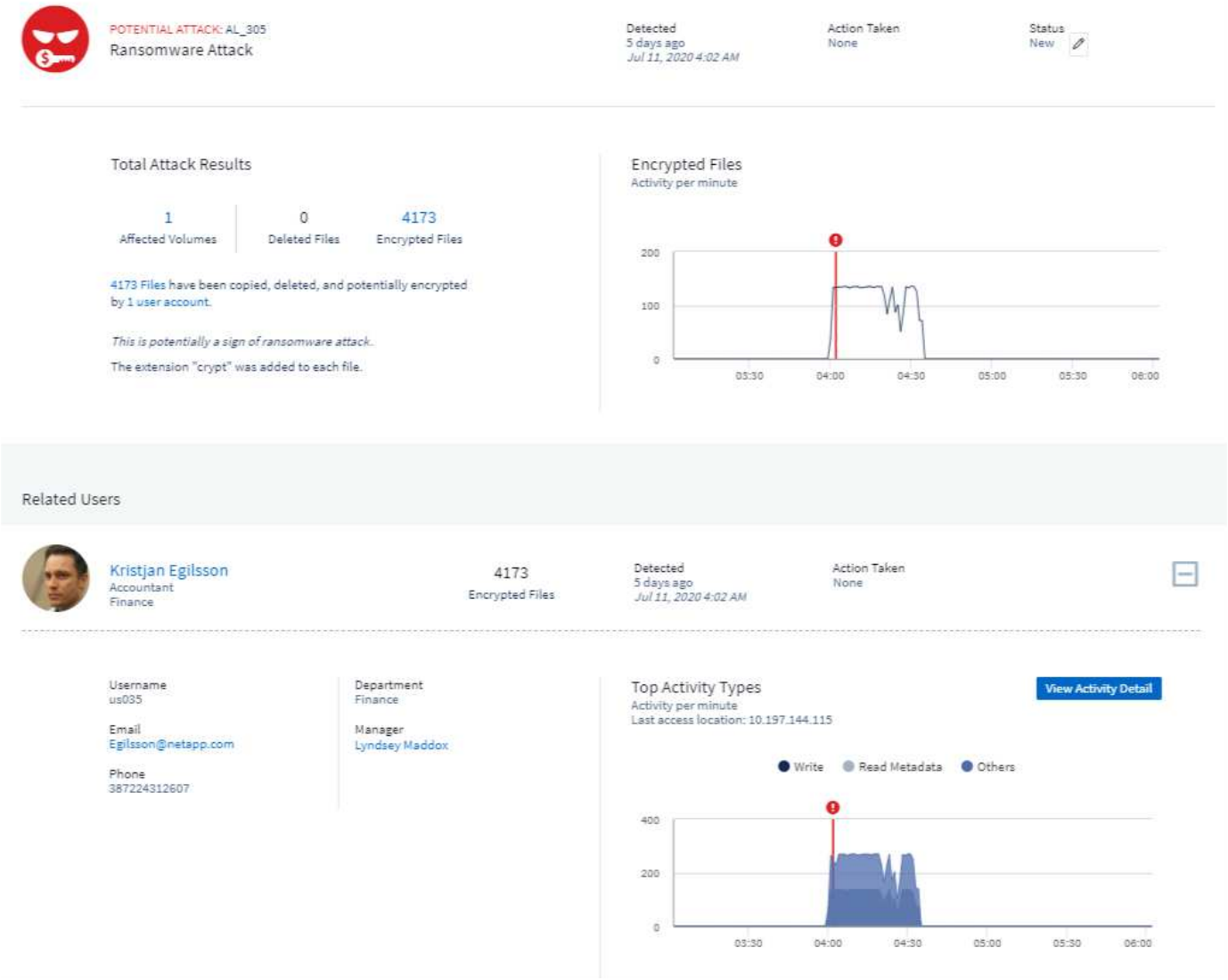
Sezione Utenti correlati:

Questa sezione mostra i dettagli sull'utente coinvolto nel potenziale attacco, incluso un grafico delle principali attività dell'utente.

Pagina degli avvisi (questo esempio mostra un potenziale attacco di manomissione dei file):



Pagina dei dettagli (questo esempio mostra un potenziale attacco di manomissione dei file):

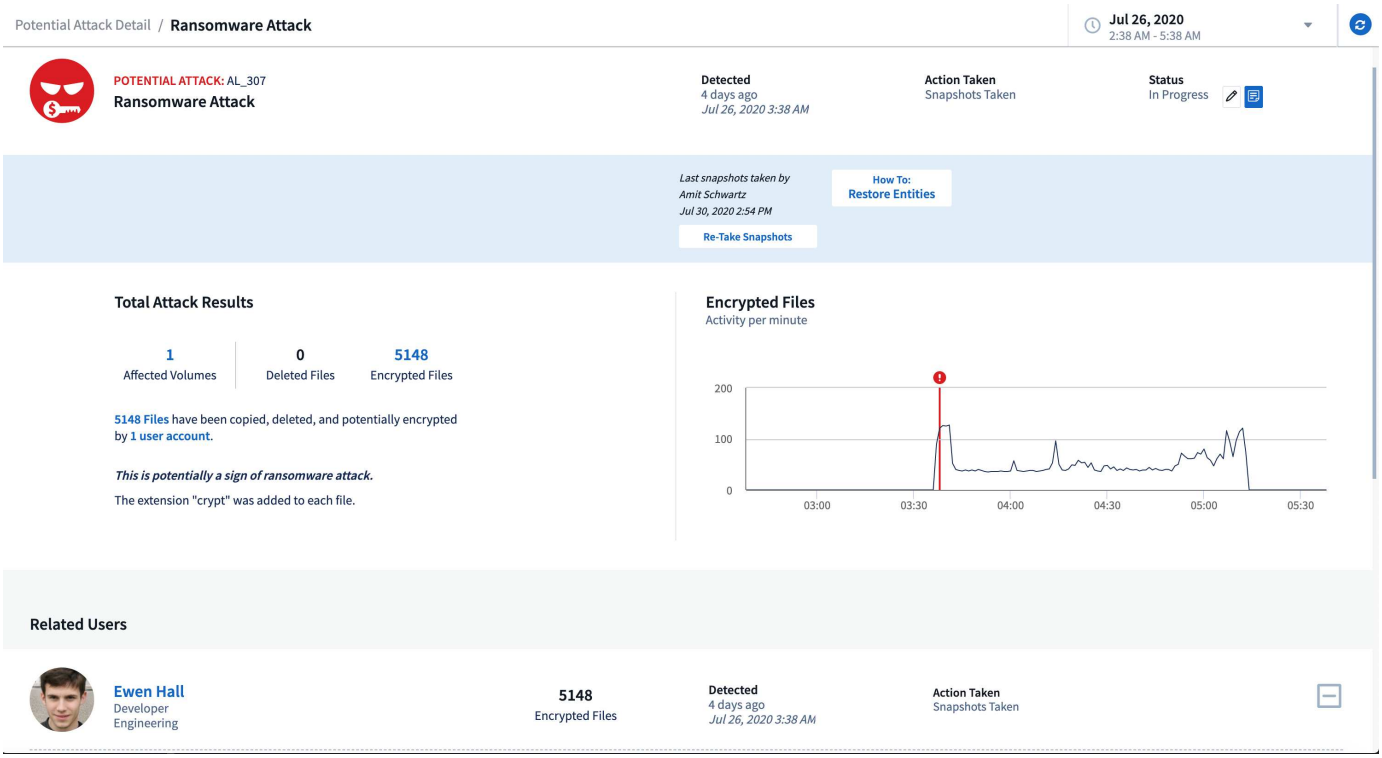


Scatta un'istantanea **Azione**

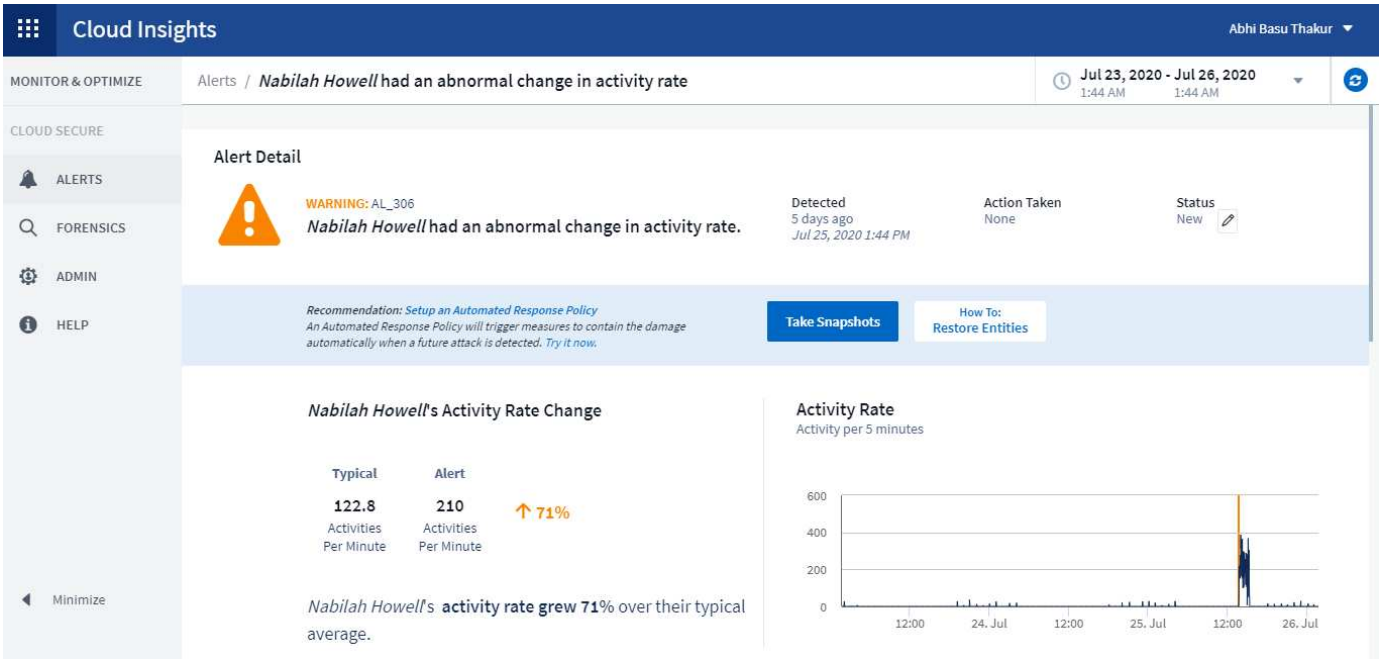
Workload Security protegge i tuoi dati eseguendo automaticamente uno snapshot quando viene rilevata un'attività dannosa, garantendo così che i tuoi dati vengano sottoposti a backup in modo sicuro.

Puoi definire "politiche di risposta automatizzate" che scattano un'istantanea quando viene rilevato un attacco di manomissione dei file o altre attività anomale dell'utente. È anche possibile acquisire manualmente uno snapshot dalla pagina di avviso.

Istantanea automatica
scattata:



Istantanea manuale:



Notifiche di avviso

Le notifiche e-mail degli avvisi vengono inviate a un elenco di destinatari degli avvisi per ogni azione sull'avviso. Per configurare i destinatari degli avvisi, fare clic su **Amministrazione > Notifiche** e immettere un indirizzo e-mail per ciascun destinatario.

Politica di conservazione

Gli avvisi e le segnalazioni vengono conservati per 13 mesi. Gli avvisi e le segnalazioni più vecchi di 13 mesi

verranno eliminati. Se l'ambiente Workload Security viene eliminato, vengono eliminati anche tutti i dati associati all'ambiente.

Risoluzione dei problemi

Problema:	Prova questo:
Esiste una situazione in cui ONTAP acquisisce snapshot orari al giorno. Gli snapshot di Workload Security (WS) avranno ripercussioni? Lo snapshot WS sostituirà lo snapshot orario? Lo snapshot orario predefinito verrà interrotto?	Gli snapshot di Workload Security non influiranno sugli snapshot orari. Gli snapshot WS non occuperanno lo spazio degli snapshot orari e la situazione dovrebbe continuare come prima. Lo snapshot orario predefinito non verrà interrotto.
Cosa succede se viene raggiunto il numero massimo di snapshot in ONTAP?	Se viene raggiunto il numero massimo di snapshot, l'acquisizione successiva degli snapshot non riuscirà e Workload Security mostrerà un messaggio di errore che indica che lo snapshot è pieno. L'utente deve definire criteri di snapshot per eliminare gli snapshot più vecchi, altrimenti gli snapshot non verranno acquisiti. In ONTAP 9.3 e versioni precedenti, un volume può contenere fino a 255 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume può contenere fino a 1023 copie Snapshot. Consultare la documentazione ONTAP per informazioni su"impostazione della politica di eliminazione degli snapshot" .
Workload Security non è in grado di acquisire snapshot.	Assicurarsi che il ruolo utilizzato per creare snapshot abbia il collegamento: https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [diritti appropriati assegnati]. Assicurarsi che *csrole* sia stato creato con i diritti di accesso appropriati per l'acquisizione di snapshot: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Gli snapshot non funzionano per gli avvisi più vecchi sulle SVM che sono state rimosse da Workload Security e successivamente aggiunte di nuovo. Per i nuovi avvisi che si verificano dopo aver aggiunto nuovamente SVM, vengono creati degli snapshot.	Si tratta di uno scenario raro. Nel caso in cui si verifichi questo problema, accedere a ONTAP ed eseguire manualmente gli snapshot per gli avvisi più vecchi.
Nella pagina *Dettagli avviso*, sotto il pulsante *Acquisisci istantanea* viene visualizzato il messaggio di errore "Ultimo tentativo fallito". Passando il mouse sopra l'errore viene visualizzato il messaggio "Il comando Invoke API è scaduto per il raccoglitore dati con ID".	Ciò può accadere quando un data collector viene aggiunto a Workload Security tramite SVM Management IP, se il LIF dell'SVM è nello stato *disabilitato* in ONTAP. Abilitare il LIF specifico in ONTAP e attivare *Esegui snapshot manualmente* da Workload Security. L'azione Snapshot avrà quindi esito positivo.

Medicina legale

Analisi forense - Tutte le attività

La pagina Tutte le attività consente di comprendere le azioni eseguite sulle entità nell'ambiente Workload Security.

Esame di tutti i dati di attività

Fare clic su **Forensics > Activity Forensics** e quindi sulla scheda **Tutte le attività** per accedere alla pagina Tutte le attività. Questa pagina fornisce una panoramica delle attività svolte sul tuo inquilino, evidenziando le seguenti informazioni:

- Un grafico che mostra la *cronologia delle attività* (in base all'intervallo di tempo globale selezionato)

  È possibile ingrandire il grafico trascinando un rettangolo al suo interno. Verrà caricata l'intera pagina per visualizzare l'intervallo di tempo ingrandito. Quando si esegue lo zoom avanti, viene visualizzato un pulsante che consente all'utente di rimpicciolire.

- Un elenco dei dati di *Tutte le attività*.
- Un menu a discesa "Raggruppa per" fornirà l'opzione di raggruppare l'attività in base a utenti, cartelle, tipo di entità, ecc.
- Un pulsante di percorso comune sarà disponibile sopra la tabella, cliccando sul quale potremo ottenere un pannello scorrevole con i dettagli del percorso dell'entità.

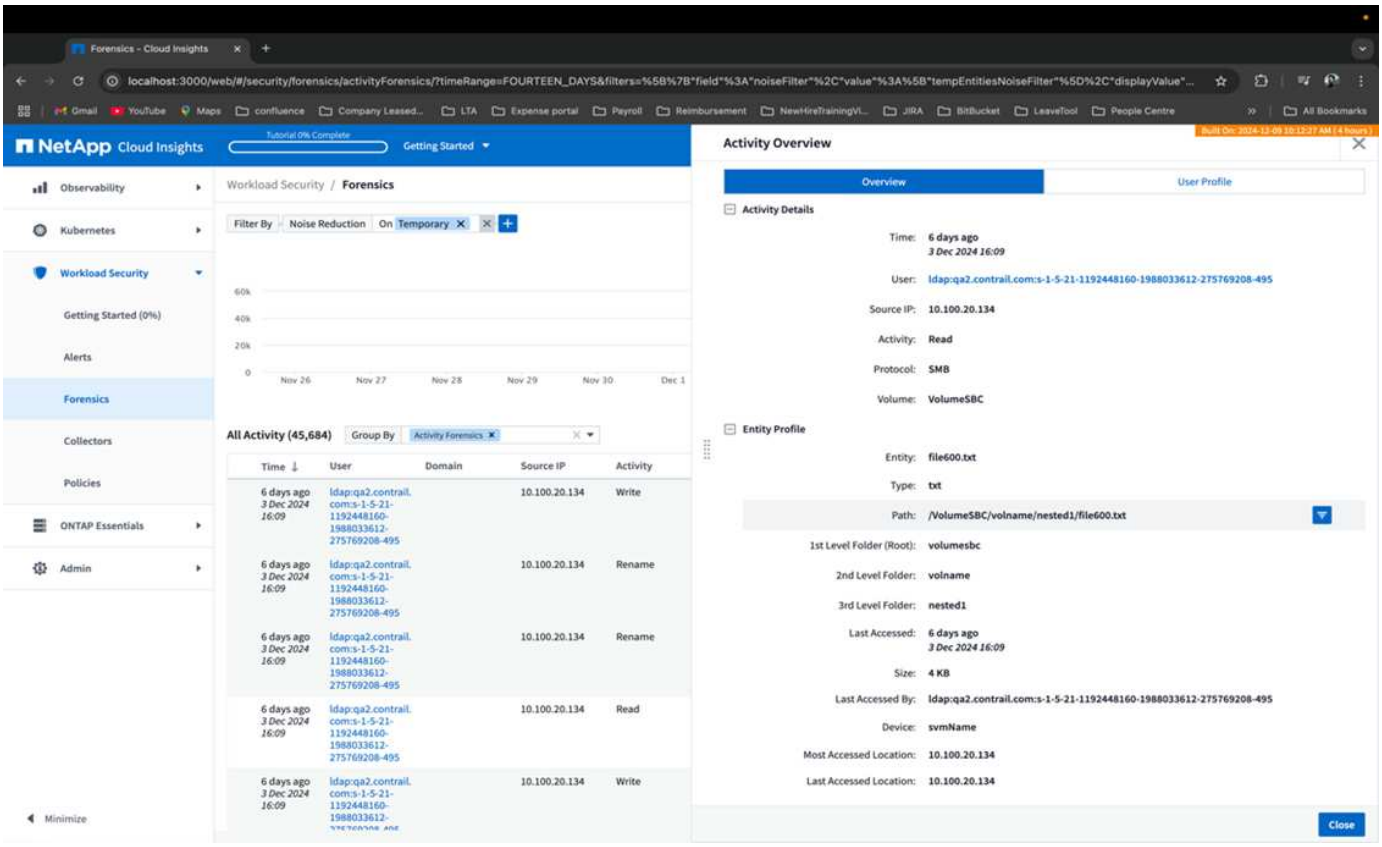
La tabella **Tutte le attività** mostra le seguenti informazioni. Si noti che non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare cliccando sull'icona "ingranaggio".

- **Ora** in cui è stato effettuato l'accesso a un'entità, inclusi anno, mese, giorno e ora dell'ultimo accesso.
- L'**utente** che ha avuto accesso all'entità con un collegamento a"Informazioni utente" come pannello scorrevole.
- L'**attività** svolta dall'utente. I tipi supportati sono:
  - **Modifica proprietà del gruppo** - La proprietà del gruppo del file o della cartella è stata modificata. Per maggiori dettagli sulla proprietà del gruppo, vedere"questo collegamento."
  - **Cambia proprietario** - La proprietà del file o della cartella è stata cambiata a un altro utente.
  - **Modifica autorizzazione** - L'autorizzazione del file o della cartella è stata modificata.
  - **Crea** - Crea file o cartella.
  - **Elimina** - Elimina file o cartella. Se una cartella viene eliminata, vengono ottenuti eventi *delete* per tutti i file presenti in quella cartella e nelle sottocartelle.
  - **Lettura** - Il file è stato letto.
  - **Leggi metadati** - Solo se si abilita l'opzione di monitoraggio delle cartelle. Verrà generato all'apertura di una cartella su Windows o eseguendo "ls" all'interno di una cartella su Linux.
  - **Rinomina** - Rinomina file o cartella.
  - **Scrittura** - I dati vengono scritti in un file.
  - **Scrivi metadati** - I metadati del file vengono scritti, ad esempio, se è stata modificata l'autorizzazione.
  - **Altro cambiamento** - Qualsiasi altro evento non descritto sopra. Tutti gli eventi non mappati vengono mappati al tipo di attività "Altra modifica". Applicabile a file e cartelle.
- Il **Percorso** è il percorso dell'*entità*. Dovrebbe essere il percorso esatto dell'entità (ad esempio,

"*/home/userX/nested1/nested2/abc.txt*") OPPURE la parte di directory del percorso per la ricerca ricorsiva (ad esempio, "*/home/userX/nested1/nested2/*"). NOTA: i modelli di percorso regex (ad esempio, *nested*) NON sono consentiti qui. In alternativa, è possibile specificare anche filtri individuali a livello di cartella del percorso, come indicato di seguito, per il filtraggio del percorso.

- La **Cartella di 1° livello (Radice)** è la directory radice del percorso dell'entità in minuscolo.
- La **Cartella di secondo livello** è la directory di secondo livello del percorso dell'entità in minuscolo.
- La **Cartella di terzo livello** è la directory di terzo livello del percorso dell'entità in minuscolo.
- La **Cartella di 4° livello** è la directory di quarto livello del percorso dell'entità in minuscolo.
- **Tipo di entità**, inclusa l'estensione dell'entità (ad esempio file) (.doc, .docx, .tmp, ecc.).
- Il **Dispositivo** in cui risiedono le entità.
- Il **Protocollo** utilizzato per recuperare gli eventi.
- Il **Percorso originale** utilizzato per gli eventi di ridenominazione quando il file originale è stato rinominato. Per impostazione predefinita, questa colonna non è visibile nella tabella. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- Il **Volume** in cui risiedono le entità. Per impostazione predefinita, questa colonna non è visibile nella tabella. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- **Nome entità** è l'ultimo componente del percorso dell'entità; per il tipo di entità come file, è il nome del file.

Selezionando una riga della tabella si apre un pannello scorrevole con il profilo utente in una scheda e la panoramica delle attività e delle entità in un'altra scheda.



Il metodo *Raggruppa per* predefinito è *Attività forense*. Se si seleziona un metodo *Raggruppa per* diverso, ad esempio Tipo di entità, verrà visualizzata la tabella *Raggruppa per* dell'entità. Se non viene effettuata alcuna selezione, viene visualizzato *Raggruppa per* **tutto**.

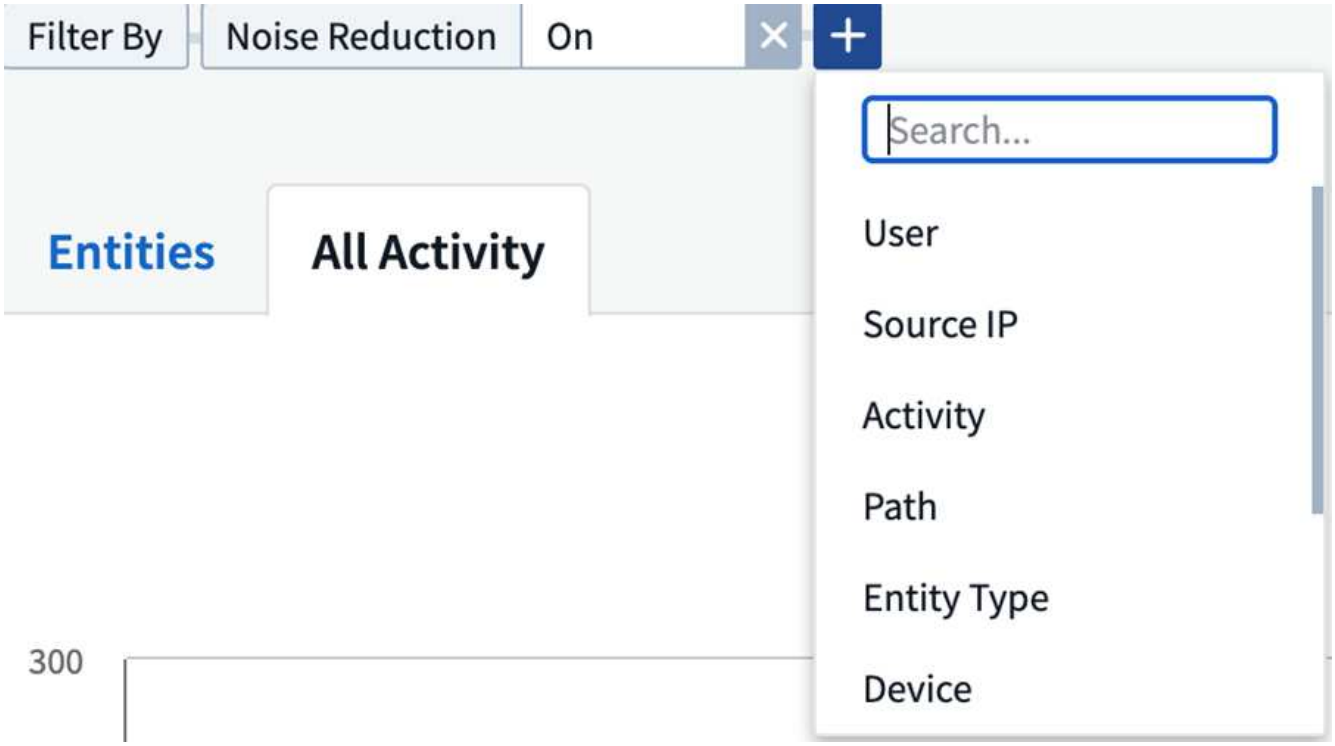
- Il conteggio delle attività viene visualizzato come collegamento ipertestuale; selezionando questa opzione, il raggruppamento selezionato verrà aggiunto come filtro. La tabella delle attività verrà aggiornata in base a quel filtro.
- Tieni presente che se modifichi il filtro, modifichi l'intervallo di tempo o aggiorni la schermata, non potrai tornare ai risultati filtrati senza impostare nuovamente il filtro.
- Si noti che quando si seleziona Nome entità come filtro, il menu a discesa Raggruppa per sarà disabilitato; inoltre, quando l'utente si trova già nella schermata Raggruppa per, il filtro Nome entità sarà disabilitato.

Filtraggio dei dati della cronologia delle attività forensi

Esistono due metodi per filtrare i dati.

- Il filtro può essere aggiunto dal pannello scorrevole. Il valore viene aggiunto ai filtri appropriati nell'elenco *Filtra per* in alto.
- Filtra i dati digitando nel campo *Filtra per*:

  Seleziona il filtro appropriato dal widget in alto "Filtra per" cliccando sul pulsante **[+]**:



  Inserisci il testo da cercare

  Premere Invio o fare clic all'esterno della casella del filtro per applicare il filtro.

È possibile filtrare i dati delle attività forensi in base ai seguenti campi:

- Il tipo **Attività**.
- **Protocollo** per recuperare attività specifiche del protocollo.
- **Nome utente** dell'utente che esegue l'attività. Per filtrare è necessario fornire il nome utente esatto. La ricerca con nome utente parziale o con nome utente parziale preceduto o suffisso '*' non funzionerà.
- **Riduzione rumore** per filtrare i file creati nelle ultime 2 ore dall'utente. Viene utilizzato anche per filtrare i

file temporanei (ad esempio, i file .tmp) a cui accede l'utente.

- **Dominio** dell'utente che esegue l'attività. Per filtrare è necessario fornire il **dominio esatto**. La ricerca di domini parziali o di domini parziali con prefisso o suffisso con carattere jolly ('*') non funzionerà. È possibile specificare *None* per cercare il dominio mancante.

I seguenti campi sono soggetti a regole di filtraggio speciali:

- **Tipo di entità**, utilizzando l'estensione dell'entità (file): è preferibile specificare il tipo di entità esatto tra virgolette. Ad esempio *"txt"*.
- **Percorso** dell'entità: deve essere il percorso esatto dell'entità (ad esempio, "*/home/userX/nested1/nested2/abc.txt*") OPPURE la parte di directory del percorso per la ricerca ricorsiva (ad esempio, "*/home/userX/nested1/nested2/*"). NOTA: i modelli di percorso regex (ad esempio, *nested*) NON sono consentiti qui. Per risultati più rapidi, si consiglia di utilizzare filtri del percorso della directory (stringa del percorso che termina con /) fino a 4 directory di profondità. Ad esempio, "*/home/userX/nested1/nested2/*". Per maggiori dettagli, consultare la tabella sottostante.
- Cartella di 1° livello (radice): directory radice dell'entità Percorso come filtri. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare home OPPURE "home".
- Cartella di 2° livello: directory di 2° livello dei filtri del percorso dell'entità. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare userX OPPURE "userX".
- Cartella di 3° livello: directory di 3° livello dei filtri del percorso dell'entità.
- Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare nested1 OPPURE "nested1".
- Cartella di 4° livello - Directory Directory di 4° livello dei filtri del percorso dell'entità. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare nested2 OPPURE "nested2".
- **Utente** che esegue l'attività: è preferibile specificare l'utente esatto tra virgolette. Ad esempio, *"Amministratore"*.
- **Dispositivo** (SVM) in cui risiedono le entità
- **Volume** in cui risiedono le entità
- Il **Percorso originale** utilizzato per gli eventi di ridenominazione quando il file originale è stato rinominato.
- **IP di origine** da cui è stato effettuato l'accesso all'entità.
  - È possibile utilizzare i caratteri jolly * e ?. Ad esempio: 10.0.0.**, 10.0?.0.10, 10.10**
  - Se è richiesta una corrispondenza esatta, è necessario fornire un indirizzo IP sorgente valido tra virgolette doppie, ad esempio "10.1.1.1.". Gli IP incompleti con virgolette doppie come "10.1.1.", "10.1..*", ecc. non funzioneranno.
- **Nome entità**: il nome del file del percorso dell'entità come filtro. Ad esempio, se il percorso dell'entità è /home/userX/nested1/testfile.txt, il nome dell'entità sarà testfile.txt. Si prega di notare che si consiglia di specificare il nome esatto del file tra virgolette; cercare di evitare le ricerche con caratteri jolly. Ad esempio, "testfile.txt". Si noti inoltre che questo filtro per nome entità è consigliato per intervalli di tempo più brevi (fino a 3 giorni).

I campi precedenti sono soggetti a quanto segue durante il filtraggio:

- Il valore esatto deve essere racchiuso tra virgolette: Esempio: "searchtext"
- Le stringhe jolly non devono contenere virgolette: Esempio: searchtext, *searchtext*, filtrerà tutte le stringhe contenenti 'searchtext'.
- Stringa con un prefisso, ad esempio: searchtext* , cercherà tutte le stringhe che iniziano con 'searchtext'.

Si prega di notare che tutti i campi filtro sono di ricerca senza distinzione tra maiuscole e minuscole. Ad esempio: se il filtro applicato è Tipo di entità con valore come 'searchtext', restituirà risultati con Tipo di entità come 'searchtext', 'SearchText', 'SEARCHTEXT'

Esempi di filtri forensi per l'attività:

Espressione del filtro applicata dall'utente	Risultato atteso	Valutazione delle prestazioni	Commento
Percorso = "/home/utenteX/nested1/nested2/"	Ricerca ricorsiva di tutti i file e le cartelle nella directory specificata	Veloce	Le ricerche nelle directory fino a 4 directory saranno rapide.
Percorso = "/home/utenteX/nested1/"	Ricerca ricorsiva di tutti i file e le cartelle nella directory specificata	Veloce	Le ricerche nelle directory fino a 4 directory saranno rapide.
Percorso = "/home/userX/nested1/test"	Corrispondenza esatta in cui il valore del percorso corrisponde a /home/userX/nested1/test	Più lentamente	La ricerca esatta sarà più lenta rispetto alle ricerche nella directory.
Percorso = "/home/utenteX/nested1/nested2/nested3/"	Ricerca ricorsiva di tutti i file e le cartelle nella directory specificata	Più lentamente	Le ricerche su più di 4 directory risultano più lente.
Qualsiasi altro filtro non basato sul percorso. Si consiglia di racchiudere i filtri di tipo utente ed entità tra virgolette, ad esempio Utente="Amministratore" Tipo di entità="txt"		Veloce	
Nome entità = "test.log"	Corrispondenza esatta in cui il nome del file è test.log	Veloce	Poiché è una corrispondenza esatta
Nome entità = *test.log	Nomi di file che terminano con test.log	Lento	A causa della wild card, può essere lento.
Nome entità = test*.log	I nomi dei file iniziano con test e terminano con .log	Lento	A causa della wild card, può essere lento.
Nome entità = test.lo	Nomi di file che iniziano con test.lo Ad esempio: corrisponderà a test.log, test.log.1, test.log1	Più lentamente	A causa della wild card alla fine, il gioco può risultare lento.
Nome entità = test	Nomi di file che iniziano con test	Il più lento	A causa della presenza di un carattere jolly alla fine e del valore più generico utilizzato, può risultare più lento.

NOTA:

1. Il conteggio delle attività visualizzato accanto all'icona Tutte le attività viene arrotondato a 30 minuti quando

l'intervallo di tempo selezionato si estende per più di 3 giorni. Ad esempio, un intervallo di tempo dal 1° settembre alle 10:15 al 7 settembre alle 10:15 mostrerà i conteggi delle attività dal 1° settembre alle 10:00 al 7 settembre alle 10:30.

2. Allo stesso modo, le metriche di conteggio mostrate nel grafico Cronologia attività vengono arrotondate a 30 minuti quando l'intervallo di tempo selezionato si estende per più di 3 giorni.

Ordinamento dei dati della cronologia delle attività forensi

È possibile ordinare i dati della cronologia delle attività in base a *Ora, Utente, IP sorgente, Attività,*, *Tipo di entità*, Cartella di 1° livello (radice), Cartella di 2° livello, Cartella di 3° livello e Cartella di 4° livello. Per impostazione predefinita, la tabella è ordinata in base all'ordine decrescente *Time*, ovvero i dati più recenti verranno visualizzati per primi. L'ordinamento è disabilitato per i campi *Dispositivo* e *Protocollo*.

Guida utente per le esportazioni asincrone

Panoramica

La funzionalità Esportazioni asincrone di Storage Workload Security è progettata per gestire esportazioni di dati di grandi dimensioni.

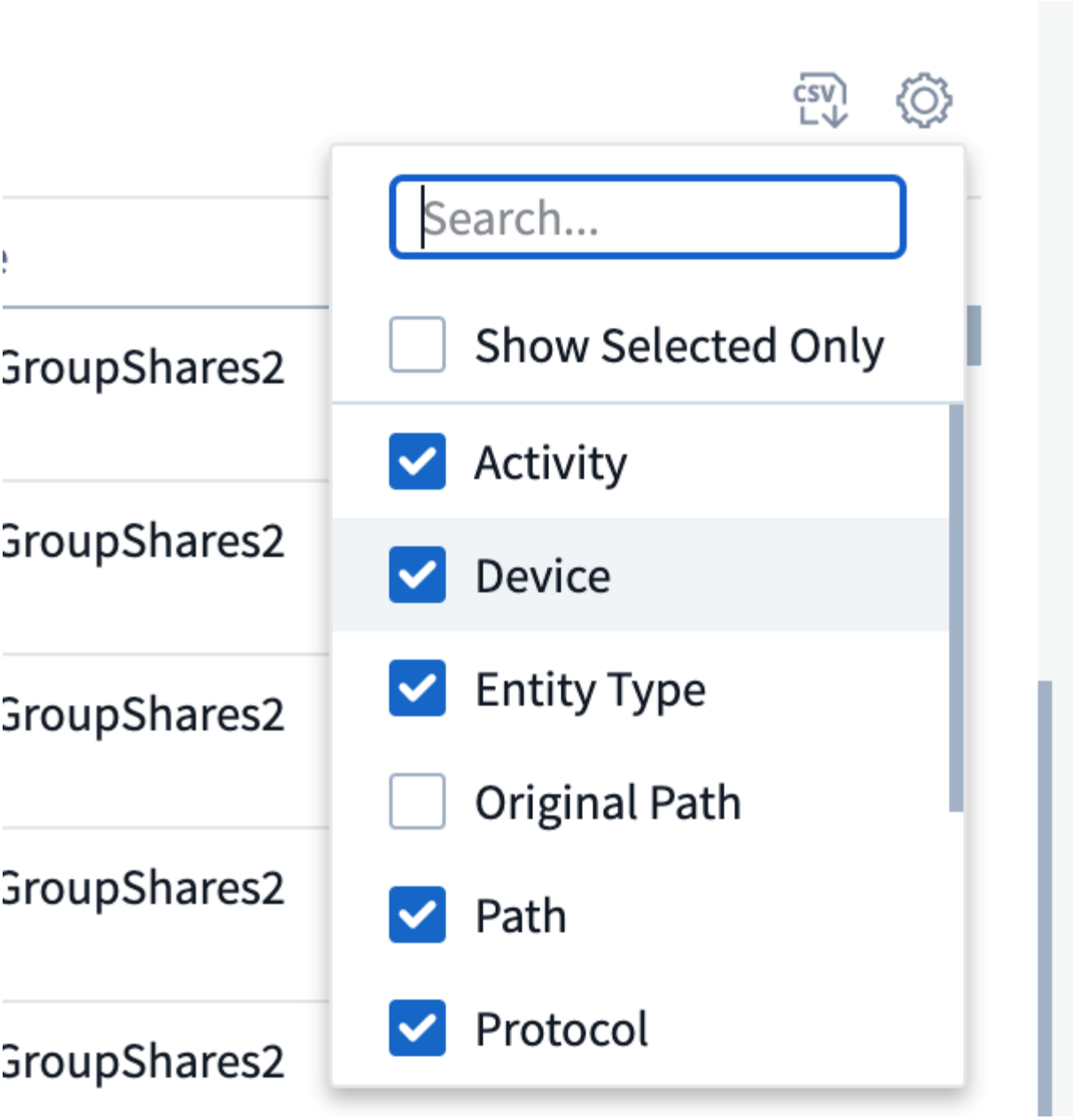
Guida passo passo: esportazione di dati con esportazioni asincrone

1. **Avvia esportazione**: seleziona la durata e i filtri desiderati per l'esportazione e fai clic sul pulsante Esporta.
2. **Attendi il completamento dell'esportazione**: il tempo di elaborazione può variare da pochi minuti ad alcune ore. Potrebbe essere necessario aggiornare la pagina forense più volte. Una volta completato il processo di esportazione, verrà abilitato il pulsante "Scarica l'ultimo file CSV esportato".
3. **Download**: Fare clic sul pulsante "Scarica l'ultimo file di esportazione creato" per ottenere i dati esportati in formato .zip. Questi dati saranno disponibili per il download finché l'utente non avvierà un'altra esportazione asincrona o finché non saranno trascorsi 3 giorni, a seconda di quale evento si verifichi per primo. Il pulsante rimarrà abilitato finché non verrà avviata un'altra esportazione asincrona.
4. **Limitazioni**:
    - Il numero di download asincroni è attualmente limitato a 1 per utente per ogni tabella Attività e Analisi Attività e a 3 per tenant.
    - I dati esportati sono limitati a un massimo di 1 milione di record per la tabella Attività; mentre per Raggruppa per, il limite è di mezzo milione di record.

Uno script di esempio per estrarre dati forensi tramite API è presente in */opt/netapp/cloudsecure/agent/export-script/* sull'agente. Per maggiori dettagli sullo script, consultare il file readme in questa posizione.

Selezione della colonna per tutte le attività

Per impostazione predefinita, la tabella *Tutte le attività* mostra colonne selezionate. Per aggiungere, rimuovere o modificare le colonne, fare clic sull'icona dell'ingranaggio a destra della tabella e selezionare dall'elenco delle colonne disponibili.



Conservazione della cronologia delle attività

La cronologia delle attività viene conservata per 13 mesi per gli ambienti Workload Security attivi.

Applicabilità dei filtri nella pagina forense

Filtro	Cosa fa	Esempio	Applicabile per questi filtri	Non applicabile per questi filtri	Risultato
* (Asterisco)	ti permette di cercare tutto	Auto*03172022 Se il testo di ricerca contiene un trattino o un carattere di sottolineatura, fornire l'espressione tra parentesi. Ad esempio, (svm*) per la ricerca di svm-123	Utente, Tipo di entità, Dispositivo, Volume, Percorso originale, Cartella di 1° livello, Cartella di 2° livello, Cartella di 3° livello, Cartella di 4° livello, Nome entità, IP sorgente		Restituisce tutte le risorse che iniziano con "Auto" e terminano con "03172022"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	AutoSabotageUser1_03172022?	Utente, Tipo di entità, Dispositivo, Volume, Cartella di 1° livello, Cartella di 2° livello, Cartella di 3° livello, Cartella di 4° livello, Nome entità, IP sorgente		restituisce AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 e così via
O	consente di specificare più entità	AutoSabotageUser1_03172022 O AutoRansomUser4_03162022	Utente, Dominio, Tipo di entità, Percorso originale, Nome entità, IP sorgente		restituisce uno qualsiasi tra AutoSabotageUser1_03172022 O AutoRansomUser4_03162022
NON	consente di escludere il testo dai risultati della ricerca	NOT AutoRansomUser4_03162022	Utente, dominio, tipo di entità, percorso originale, cartella di 1° livello, cartella di 2° livello, cartella di 3° livello, cartella di 4° livello, nome dell'entità, IP di origine	Dispositivo	restituisce tutto ciò che non inizia con "AutoRansomUser4_03162022"
Nessuno	cerca valori NULL in tutti i campi	Nessuno	Dominio		restituisce risultati in cui il campo di destinazione è vuoto

Ricerca percorso

I risultati della ricerca con e senza / saranno diversi

"/AutoDir1/AutoFile03242022"	Funziona solo la ricerca esatta; restituisce tutte le attività con percorso esatto come /AutoDir1/AutoFile03242022 (senza distinzione tra maiuscole e minuscole)
"/AutoDir1/ "	Funziona; restituisce tutte le attività con directory di primo livello corrispondente ad AutoDir1 (senza distinzione tra maiuscole e minuscole)
"/AutoDir1/AutoFile03242022/"	Funziona; restituisce tutte le attività con la directory di 1° livello corrispondente ad AutoDir1 e la directory di 2° livello corrispondente ad AutoFile03242022 (senza distinzione tra maiuscole e minuscole)
/AutoDir1/AutoFile03242022 OPPURE /AutoDir1/AutoFile03242022	Non funziona
NON /AutoDir1/AutoFile03242022	Non funziona
NON /AutoDir1	Non funziona
NON /AutoFile03242022	Non funziona
*	Non funziona

Modifiche all'attività dell'utente SVM radice locale

Se un utente root SVM locale sta eseguendo un'attività, l'IP del client su cui è montata la condivisione NFS viene ora considerato nel nome utente, che verrà visualizzato come root@<indirizzo-ip-del-client> sia nelle pagine delle attività forensi che in quelle delle attività utente.

Per esempio:

- Se SVM-1 è monitorato da Workload Security e l'utente root di tale SVM monta la condivisione su un client con indirizzo IP 10.197.12.40, il nome utente mostrato nella pagina delle attività forensi sarà *root@10.197.12.40*.
- Se lo stesso SVM-1 viene montato su un altro client con indirizzo IP 10.197.12.41, il nome utente mostrato nella pagina delle attività forensi sarà *root@10.197.12.41*.

*• Ciò viene fatto per separare l'attività dell'utente root NFS in base all'indirizzo IP. In precedenza, tutte le attività erano considerate eseguite solo dall'utente *root*, senza distinzione di IP.

Risoluzione dei problemi

Problema	Prova questo

Nella tabella "Tutte le attività", nella colonna "Utente", il nome utente è visualizzato come: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" o "ldap:default:80038003"	Le possibili ragioni potrebbero essere: 1. Non è stato ancora configurato alcun raccoglitore di directory utente. Per aggiungerne uno, vai su **Sicurezza del carico di lavoro > Collettori > Collettori directory utente** e fai clic su **+Collettore directory utente**. Scegliere *Active Directory* o *LDAP Directory Server*. 2. È stato configurato un User Directory Collector, ma si è arrestato o è in stato di errore. Vai su **Collezionisti > Collezionisti directory utenti** e controlla lo stato. Fare riferimento al"Risoluzione dei problemi di User Directory Collector" sezione della documentazione per suggerimenti sulla risoluzione dei problemi. Dopo aver effettuato la configurazione corretta, il nome verrà risolto automaticamente entro 24 ore. Se il problema persiste, controlla di aver aggiunto il corretto User Data Collector. Assicurarsi che l'utente faccia effettivamente parte del server Active Directory/LDAP Directory aggiunto.
Alcuni eventi NFS non vengono visualizzati nell'interfaccia utente.	Controllare quanto segue: 1. Un raccoglitore di directory utente per il server AD con attributi POSIX impostati dovrebbe essere in esecuzione con l'attributo unixid abilitato dall'interfaccia utente. 2. Tutti gli utenti che effettuano l'accesso NFS dovrebbero essere visibili quando si effettua una ricerca nella pagina utente dall'interfaccia utente 3. Gli eventi non elaborati (eventi per i quali l'utente non è ancora stato individuato) non sono supportati per NFS 4. L'accesso anonimo all'esportazione NFS non verrà monitorato. 5. Assicurarsi che la versione NFS utilizzata sia la 4.1 o una versione precedente. (Si noti che NFS 4.1 è supportato con ONTAP 9.15 o versioni successive.)
Dopo aver digitato alcune lettere contenenti un carattere jolly come l'asterisco (*) nei filtri delle pagine Forensics *All Activity* o *Entities*, le pagine si caricano molto lentamente.	Un asterisco (*) nella stringa di ricerca cerca tutto. Tuttavia, l'uso di stringhe jolly iniziali come *<searchTerm>* o *<searchTerm>** causerà una query lenta. Per ottenere prestazioni migliori, utilizzare invece stringhe di prefisso nel formato <searchTerm>* (in altre parole, aggiungere l'asterisco (*) *dopo* un termine di ricerca). Esempio: utilizzare la stringa *testvolume**, anziché *testvolume* o *test*volume*. Utilizzare una ricerca di directory per visualizzare ricorsivamente tutte le attività presenti in una determinata cartella (ricerca gerarchica). Ad esempio, "/path1/path2/path3/" elencherà ricorsivamente tutte le attività presenti in /path1/path2/path3. In alternativa, utilizzare l'opzione "Aggiungi al filtro" nella scheda Tutte le attività.
Quando utilizzo un filtro Percorso, ricevo l'errore "Richiesta non riuscita con codice di stato 500/503".	Prova a utilizzare un intervallo di date più piccolo per filtrare i record.

L’interfaccia utente forense carica i dati lentamente quando si utilizza il filtro *path*.	Per risultati più rapidi, si consiglia di utilizzare filtri del percorso della directory (stringa del percorso che termina con /) fino a 4 directory di profondità. Ad esempio, se il percorso della directory è /Aaa/Bbb/Ccc/Ddd, provare a cercare "/Aaa/Bbb/Ccc/Ddd/" per caricare i dati più velocemente.
L’interfaccia utente di Forensics carica i dati lentamente e riscontra errori quando si utilizza il filtro del nome dell’entità.	Prova con intervalli di tempo più piccoli e con la ricerca del valore esatto con virgolette doppie. Ad esempio, se entityPath è "/home/userX/nested1/nested2/nested3/testfile.txt", prova con "testfile.txt" come filtro del nome dell’entità.

Panoramica utente forense

Le informazioni per ciascun utente sono fornite nella Panoramica utente. Utilizzare queste visualizzazioni per comprendere le caratteristiche degli utenti, le entità associate e le attività recenti.

Profilo utente

Le informazioni del profilo utente includono le informazioni di contatto e la posizione dell’utente. Il profilo fornisce le seguenti informazioni:

- Nome dell’utente
- Indirizzo email dell’utente
- Responsabile dell’utente
- Contatto telefonico per l’utente
- Posizione dell’utente

Comportamento dell’utente

Le informazioni sul comportamento dell’utente identificano le attività e le operazioni recenti eseguite dall’utente. Queste informazioni includono:

- Attività recenti
  - Ultimo luogo di accesso
  - Grafico delle attività
  - Avvisi
- Operazioni degli ultimi sette giorni
  - Numero di operazioni

Intervallo di aggiornamento

L’elenco degli utenti viene aggiornato ogni 12 ore.

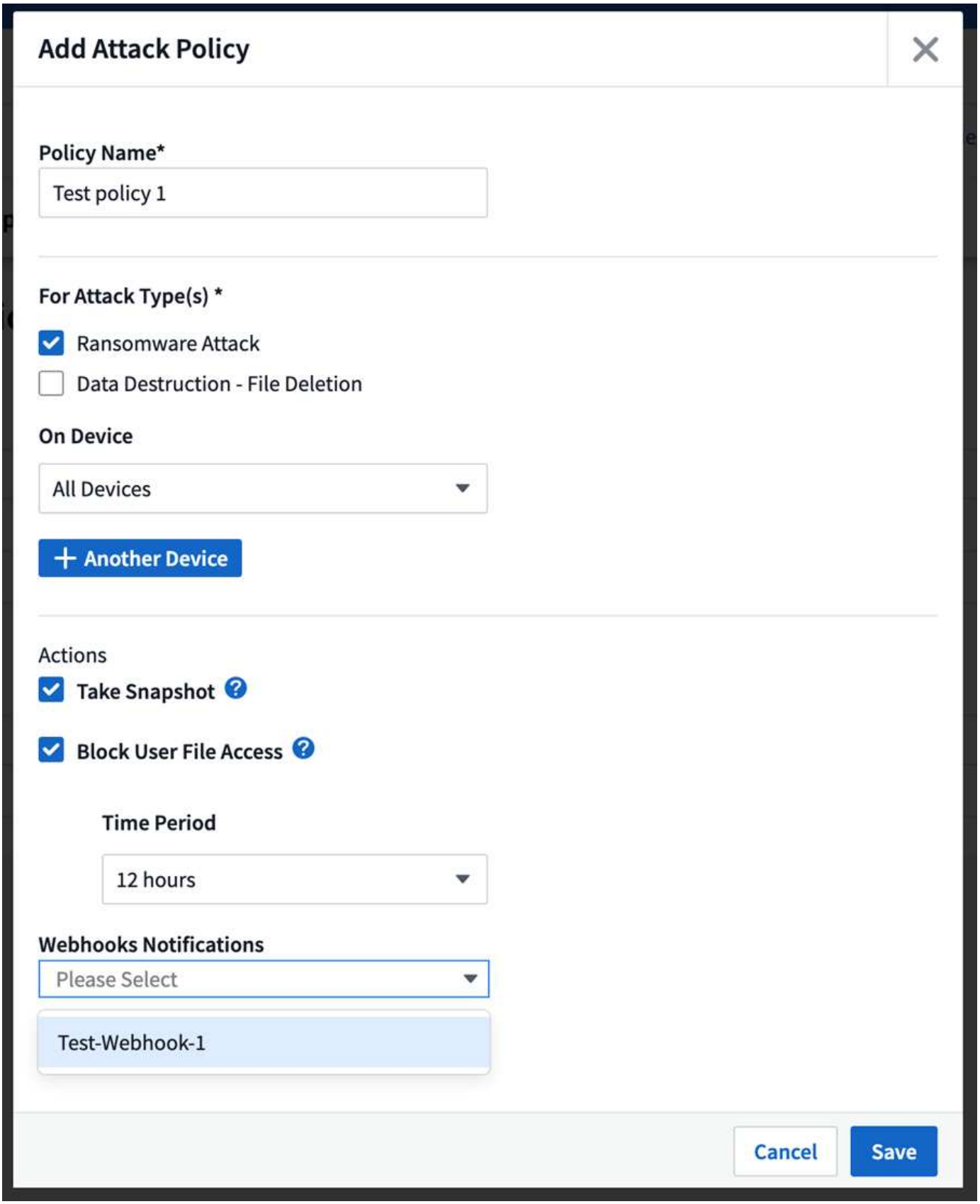
Politica di conservazione

Se non viene aggiornato nuovamente, l'elenco degli utenti viene conservato per 13 mesi. Dopo 13 mesi i dati verranno cancellati. Se l'ambiente Workload Security viene eliminato, tutti i dati associati all'ambiente vengono eliminati.

Criteri di risposta automatizzati

I criteri di risposta attivano azioni quali l'acquisizione di uno snapshot o la limitazione dell'accesso dell'utente in caso di attacco o comportamento anomalo dell'utente.

È possibile impostare criteri su dispositivi specifici o su tutti i dispositivi. Per impostare un criterio di risposta, seleziona **Amministrazione > Criteri di risposta automatica** e fai clic sul pulsante **+Criterio** appropriato. È possibile creare policy per gli attacchi o per gli avvisi.



È necessario salvare la policy con un nome univoco.

Per disattivare un'azione di risposta automatica (ad esempio, Acquisisci snapshot), è sufficiente deselezionare l'azione e salvare il criterio.

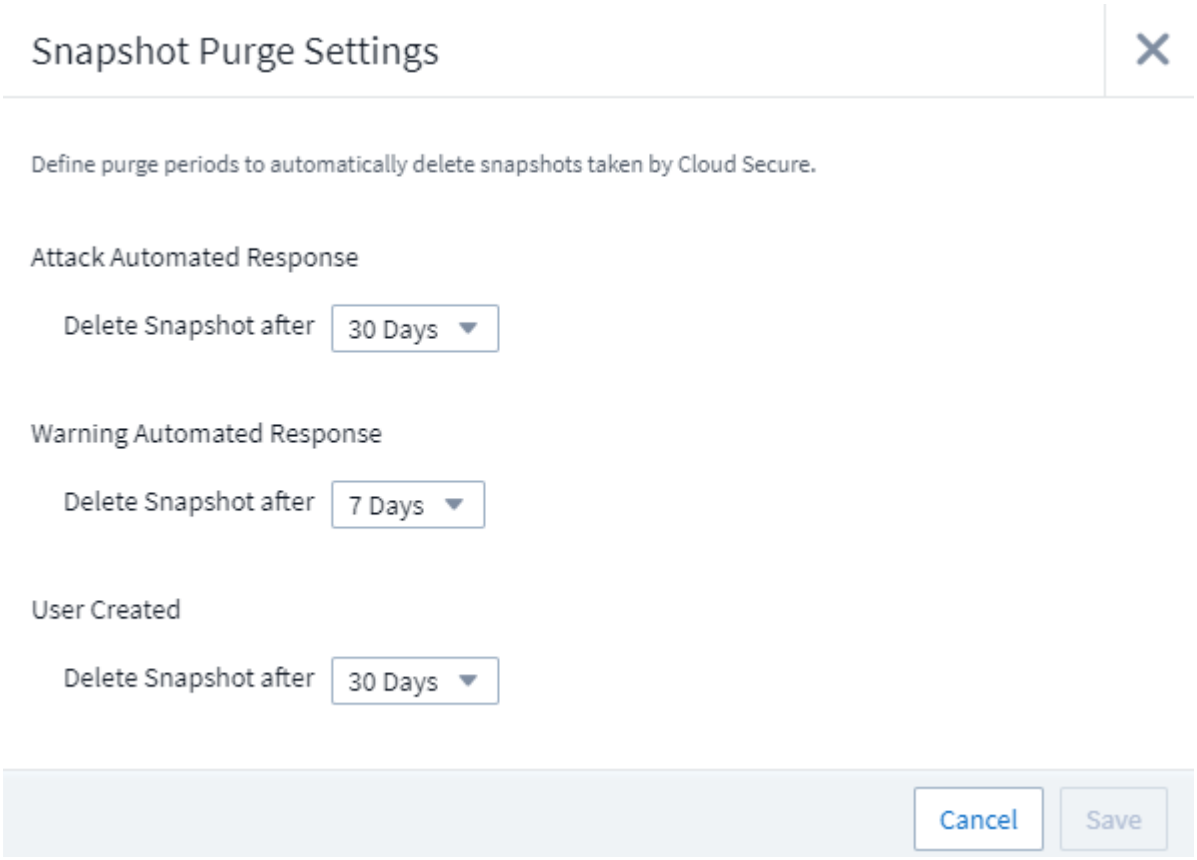
Quando viene attivato un avviso sui dispositivi specificati (o su tutti i dispositivi, se selezionati), il criterio di risposta automatica acquisisce un'istantanea dei dati. È possibile visualizzare lo stato dell'istantanea su"Pagina dei dettagli dell'avviso" .

Vedi il"Limita l'accesso degli utenti" pagina per maggiori dettagli sulla limitazione dell'accesso degli utenti tramite IP.

È possibile allegare uno o più webhook a un criterio per ricevere una notifica quando viene creato un avviso e viene intrapresa un'azione. Si consiglia di aggiungere non più di 10 webhook a una policy. Tenere presente che se una policy viene sospesa, le notifiche webhook non verranno attivate.

È possibile modificare o sospendere una policy di risposta automatica selezionando l'opzione nel menu a discesa della policy.

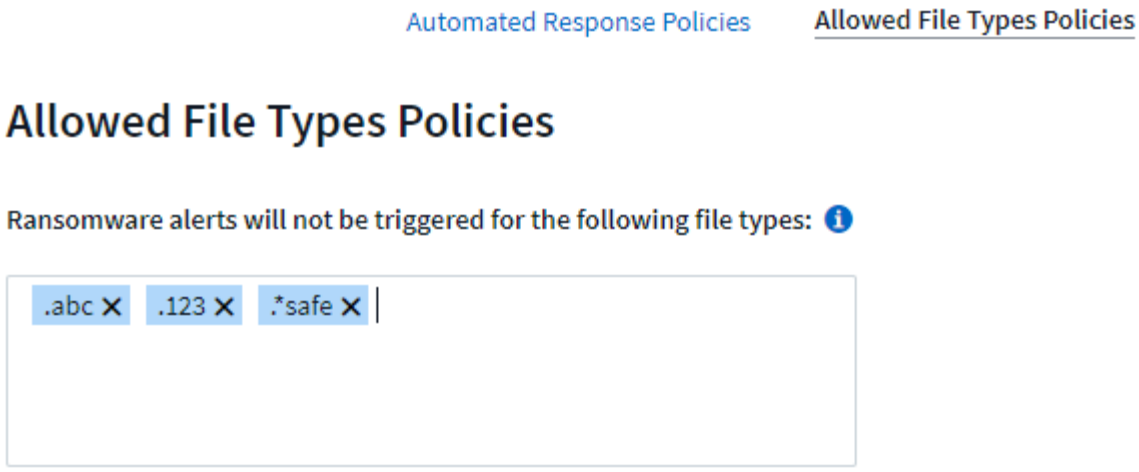
Workload Security eliminerà automaticamente gli snapshot una volta al giorno in base alle impostazioni di Snapshot Purge.



Criteri sui tipi di file consentiti

Se viene rilevato un attacco di manomissione di un file per un'estensione di file nota e vengono generati avvisi nella schermata Avvisi, è possibile aggiungere tale estensione di file a un elenco di *tipi di file consentiti* per evitare avvisi non necessari.

Passare a **Sicurezza del carico di lavoro > Criteri** e andare alla scheda *Criteri sui tipi di file consentiti*.



Una volta aggiunto all'elenco dei *tipi di file consentiti*, non verrà generato alcun avviso di attacco di manomissione dei file per quel tipo di file consentito. Si noti che la politica *Tipi di file consentiti* è applicabile solo per il rilevamento di manomissioni di file.

Ad esempio, se un file denominato *test.txt* viene rinominato in *test.txt.abc* e Workload Security rileva un attacco di manomissione del file a causa dell'estensione *.abc*, l'estensione *.abc* può essere aggiunta all'elenco dei *tipi di file consentiti*. Dopo l'aggiunta all'elenco, gli attacchi di manomissione dei file non verranno più generati contro i file con estensione *.abc*.

I tipi di file consentiti possono essere corrispondenze esatte (ad esempio, ".abc") o espressioni (ad esempio, "**.type", ".type**" o "**type**"). Le espressioni di tipo ".a*c", ".p*f" non sono supportate.

Integrazione con la protezione autonoma dai ransomware ONTAP

La funzionalità di protezione autonoma ONTAP utilizza l'analisi del carico di lavoro negli ambienti NAS (NFS e SMB) per rilevare in modo proattivo e segnalare attività anomale nei file che potrebbero indicare attacchi dannosi o modifiche non autorizzate dei dati.

Ulteriori dettagli e requisiti di licenza su ARP possono essere trovati"Qui" .

Workload Security si integra con ONTAP per ricevere eventi ARP e fornire un ulteriore livello di analisi e risposte automatiche.

Workload Security riceve gli eventi ARP da ONTAP ed esegue le seguenti azioni:

1. Correla gli eventi di crittografia del volume con l'attività dell'utente per identificare chi sta causando il danno.
2. Implementa politiche di risposta automatica (se definite)
3. Fornisce funzionalità forensi:
    - Consentire ai clienti di condurre indagini sulle violazioni dei dati.
    - Identificare i file interessati, contribuendo a un recupero più rapido e a condurre indagini sulle violazioni dei dati.

Prerequisiti

1. Versione minima ONTAP : 9.11.1
2. Volumi abilitati ARP. I dettagli sull'abilitazione di ARP possono essere trovati"Qui" . ARP deve essere abilitato tramite OnCommand System Manager. Workload Security non può abilitare ARP.
3. Il collettore di sicurezza del carico di lavoro deve essere aggiunto tramite l'IP del cluster.
4. Per il funzionamento di questa funzionalità sono necessarie le credenziali a livello di cluster. In altre parole, quando si aggiunge l'SVM è necessario utilizzare le credenziali a livello di cluster.

Autorizzazioni utente richieste

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni concesse all'utente, seguire i passaggi sottostanti per concedere a Workload Security le autorizzazioni per raccogliere informazioni relative ad ARP da ONTAP.

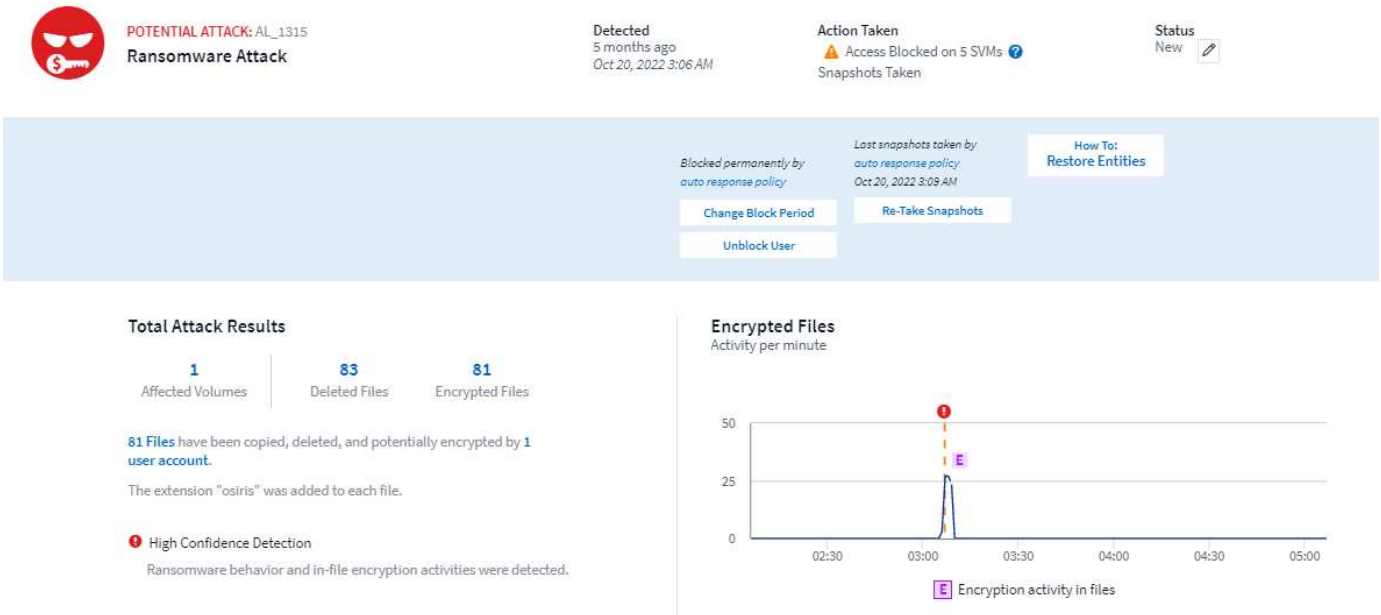
Per *csuser* con credenziali del cluster, procedere come segue dalla riga di comando ONTAP :

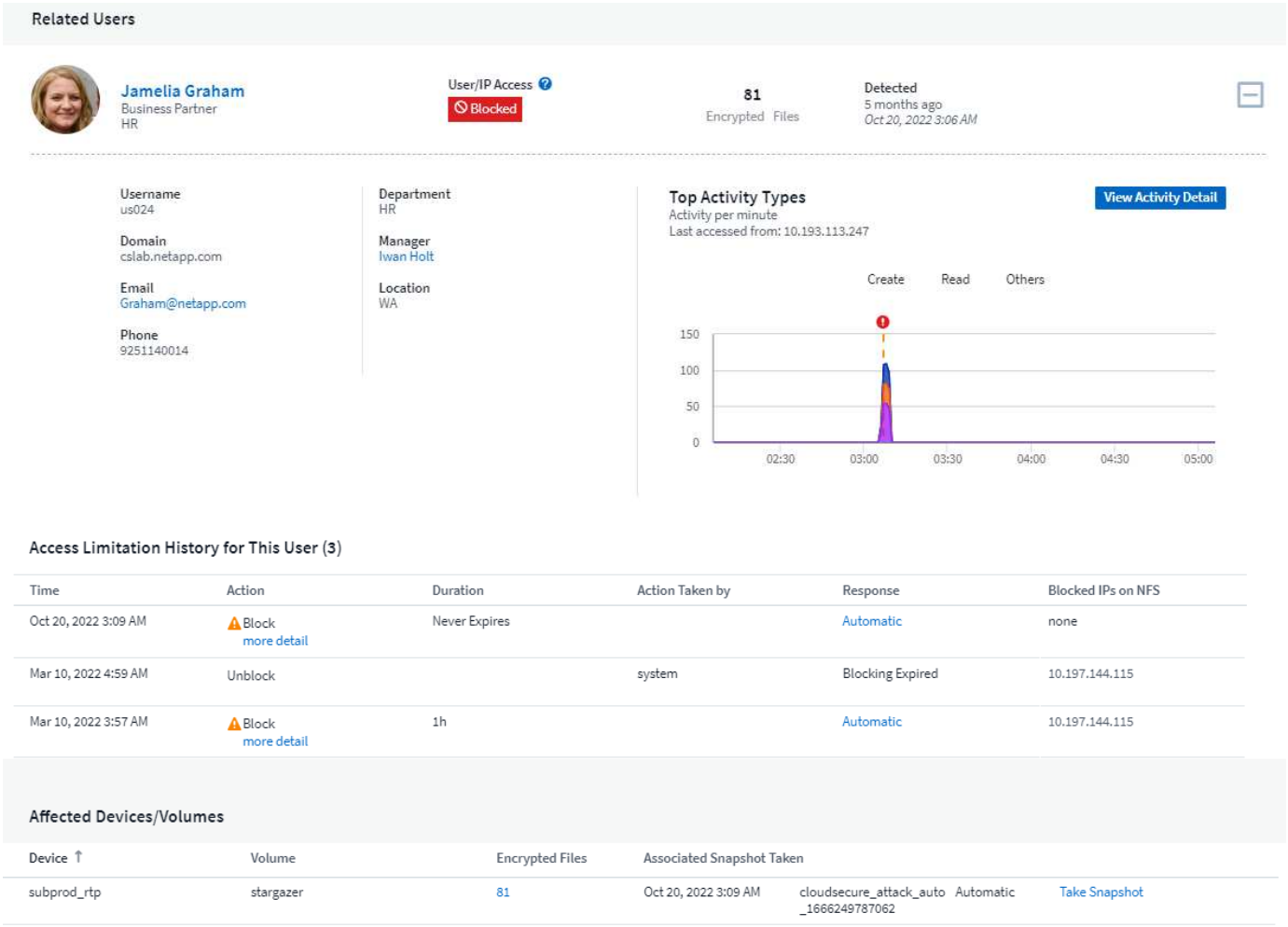
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

Per saperne di più sulla configurazione di altri"Autorizzazioni ONTAP" .

Esempio di avviso

Di seguito è riportato un esempio di avviso generato a causa di un evento ARP:





Un banner di alta affidabilità indica che l'attacco ha mostrato un comportamento di manomissione dei file insieme ad attività di crittografia dei file. Il grafico dei file crittografati indica il timestamp in cui l'attività di crittografia del volume è stata rilevata dalla soluzione ARP.

Limitazioni

Nel caso in cui un SVM non sia monitorato da Workload Security, ma vi siano eventi ARP generati da ONTAP, gli eventi verranno comunque ricevuti e visualizzati da Workload Security. Tuttavia, le informazioni forensi relative all'avviso, così come la mappatura degli utenti, non verranno acquisite o mostrate.

Risoluzione dei problemi

Nella tabella seguente sono descritti i problemi noti e le relative soluzioni.

Problema:	Risoluzione:
Gli avvisi via e-mail vengono ricevuti 24 ore dopo il rilevamento di un attacco. Nell'interfaccia utente, gli avvisi vengono visualizzati 24 ore prima che le e-mail vengano ricevute da Data Infrastructure Insights Workload Security.	Quando ONTAP invia l'evento *Ransomware Detected* a Data Infrastructure Insights Workload Security (ovvero Workload Security), l'e-mail viene inviata. L'evento contiene un elenco degli attacchi e i relativi timestamp. L'interfaccia utente di Workload Security visualizza il timestamp dell'avviso del primo file attaccato. ONTAP invia l'evento *Ransomware Detected* a Data Infrastructure Insights quando viene codificato un certo numero di file. Potrebbe quindi esserci una differenza tra l'orario in cui l'avviso viene visualizzato nell'interfaccia utente e l'orario in cui viene inviata l'e-mail.

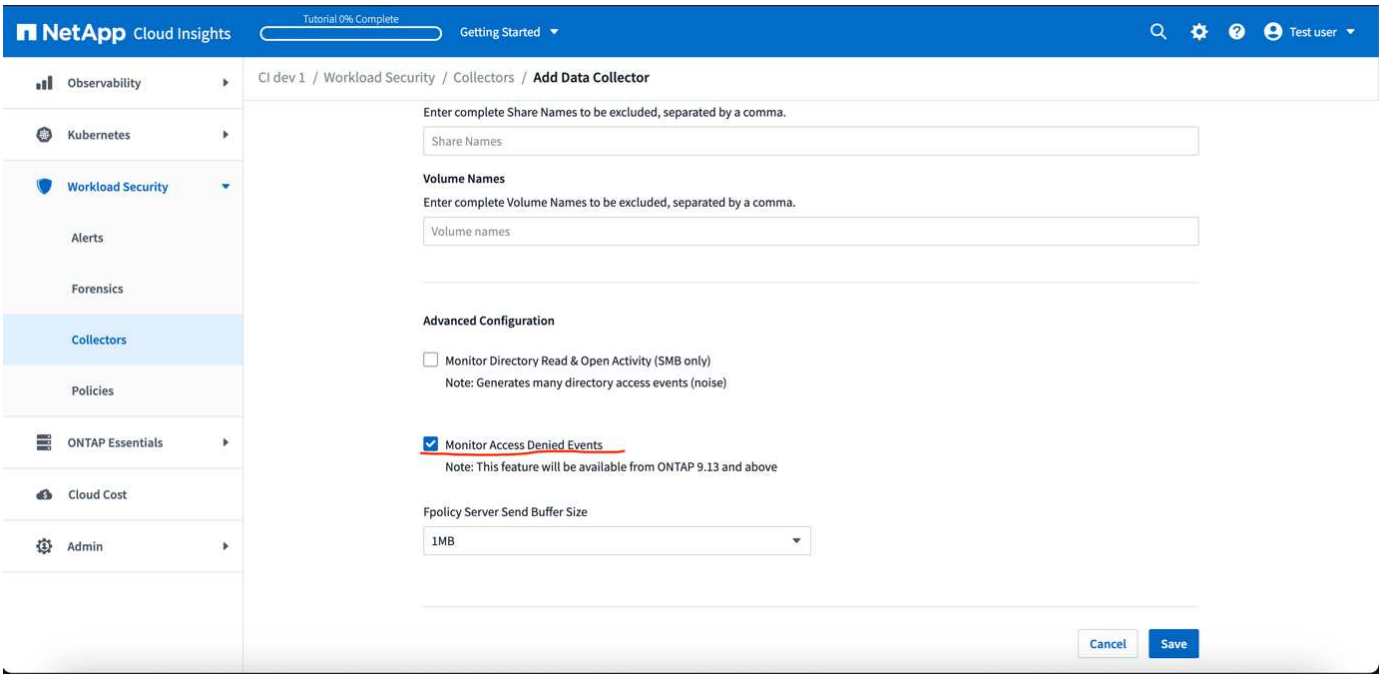
Integrazione con ONTAP Accesso negato

La funzionalità ONTAP Access Denied utilizza l'analisi del carico di lavoro negli ambienti NAS (NFS e SMB) per rilevare in modo proattivo e avvisare in caso di operazioni sui file non riuscite (ad esempio, un utente che tenta di eseguire un'operazione per la quale non ha l'autorizzazione). Queste notifiche di operazioni sui file non riuscite, soprattutto in caso di errori legati alla sicurezza, aiuteranno ulteriormente a bloccare gli attacchi interni nelle fasi iniziali.

Data Infrastructure Insights Workload Security si integra con ONTAP per ricevere eventi di accesso negato e fornire un ulteriore livello di risposta automatica e analitica.

Prerequisiti

- Versione minima ONTAP : 9.13.0.
- Un amministratore di Workload Security deve abilitare la funzionalità Accesso negato durante l'aggiunta di un nuovo collector o la modifica di un collector esistente, selezionando la casella di controllo *Monitora eventi di accesso negato* in Configurazione avanzata.



Autorizzazioni utente richieste

Se il Data Collector viene aggiunto utilizzando le credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se il Collector viene aggiunto tramite un utente personalizzato (ad esempio, *csuser*) con autorizzazioni concesse all'utente, seguire i passaggi sottostanti per concedere a Workload Security l'autorizzazione necessaria per registrarsi per gli eventi di accesso negato con ONTAP.

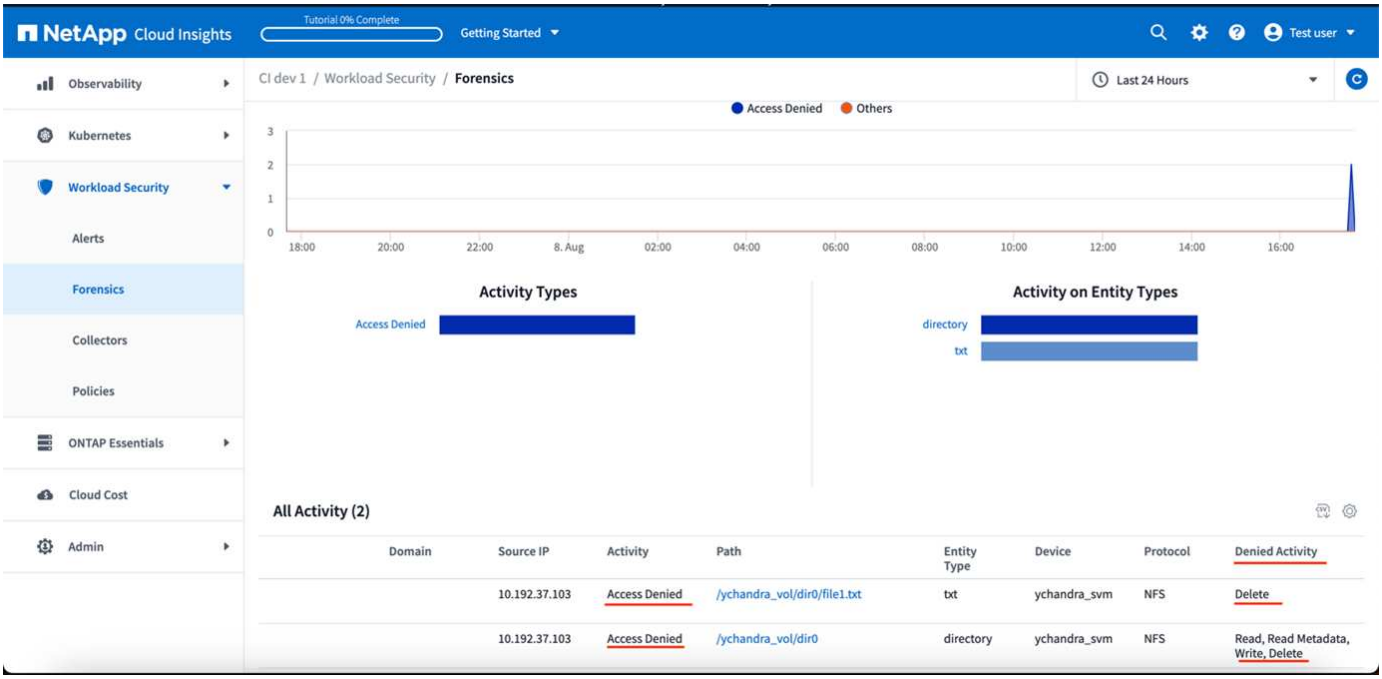
Per csuser con credenziali *cluster*, eseguire i seguenti comandi dalla riga di comando ONTAP . Si noti che questa autorizzazione potrebbe già esistere.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Per csuser con credenziali _SVM_, eseguire i seguenti comandi dalla riga
di comando ONTAP .  Si noti che questa autorizzazione potrebbe già
esistere.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
Per saperne di più sulla configurazione di
altrilink:task_add_collector_svm.html["Autorizzazioni ONTAP"] .
```

Eventi di accesso negato

Una volta acquisiti gli eventi dal sistema ONTAP , la pagina Workload Security Forensics mostrerà gli eventi di accesso negato. Oltre alle informazioni visualizzate, è possibile visualizzare le autorizzazioni utente mancanti per una particolare operazione aggiungendo la colonna *Attività desiderata* alla tabella tramite l'icona a forma di ingranaggio.



Blocco dell'accesso degli utenti per fermare gli attacchi

Interrompere immediatamente gli attacchi rilevati bloccando l'accesso degli utenti compromessi per impedire ulteriori danni ai dati o l'esfiltrazione. Workload Security consente sia il blocco automatico tramite criteri di risposta automatizzati sia l'intervento manuale dalle pagine di avviso o dei dettagli dell'utente, offrendoti un controllo flessibile sulla tua risposta di sicurezza. Le restrizioni di accesso si applicano automaticamente a tutti i volumi di archiviazione monitorati e sono limitate nel tempo per il ripristino automatico.

L'utente viene bloccato direttamente per SMB e l'indirizzo IP delle macchine host che causano l'attacco verrà bloccato per NFS. A tali indirizzi IP delle macchine verrà impedito l'accesso a qualsiasi Storage Virtual Machine (SVM) monitorata da Workload Security.

Ad esempio, supponiamo che Workload Security gestisca 10 SVM e che la politica di risposta automatica sia configurata per quattro di queste SVM. Se l'attacco ha origine in una delle quattro SVM, l'accesso dell'utente verrà bloccato in tutte e 10 le SVM. Viene comunque eseguito uno snapshot sull'SVM di origine.

Se sono presenti quattro SVM, di cui una configurata per SMB, una per NFS e le restanti due configurate sia per NFS che per SMB, tutte le SVM verranno bloccate se l'attacco ha origine in una qualsiasi delle quattro SVM.

Prerequisiti per il blocco dell'accesso utente

Per il funzionamento di questa funzionalità sono necessarie le credenziali a livello di cluster.

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni concesse all'utente, seguire i passaggi seguenti per concedere a Workload Security le autorizzazioni per bloccare l'utente.

Per csuser con credenziali cluster, procedere come segue dalla riga di comando ONTAP :

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Assicurati di rivedere la sezione Autorizzazioni del"Configurazione del raccoglitore dati ONTAP SVM" anche la pagina.

Come abilitare la funzionalità?

- In Workload Security, vai a **Workload Security > Criteri > Criteri di risposta automatica**. Seleziona **+Politica di attacco**.
- Selezionare (selezionare) *Blocca accesso file utente*.

Come impostare il blocco automatico dell'accesso degli utenti?

- Crea una nuova politica di attacco o modifica una politica di attacco esistente.
- Selezionare le SVM su cui monitorare la policy di attacco.
- Fare clic sulla casella di controllo "Blocca accesso file utente". La funzionalità verrà abilitata quando questa opzione è selezionata.
- In "Periodo di tempo" seleziona l'orario fino al quale deve essere applicato il blocco.
- Per testare il blocco automatico degli utenti, puoi simulare un attacco tramite un"sceneggiatura simulata" .

Come sapere se ci sono utenti bloccati nel sistema?

- Nella pagina degli elenchi di avvisi, verrà visualizzato un banner nella parte superiore dello schermo nel caso in cui un utente venga bloccato.
- Cliccando sul banner verrai indirizzato alla pagina "Utenti", dove potrai vedere l'elenco degli utenti bloccati.
- Nella pagina "Utenti", c'è una colonna denominata "Accesso utente/IP". In quella colonna verrà visualizzato lo stato attuale del blocco dell'utente.

Limitare e gestire manualmente l'accesso degli utenti

- È possibile accedere alla schermata dei dettagli dell'avviso o dei dettagli dell'utente e quindi bloccare o ripristinare manualmente un utente da tali schermate.

Cronologia delle limitazioni di accesso utente

Nella pagina dei dettagli dell'avviso e dei dettagli dell'utente, nel pannello utente, è possibile visualizzare un controllo della cronologia delle limitazioni di accesso dell'utente: ora, azione (blocca, sblocca), durata, azione intrapresa da, manuale/automatica e IP interessati per NFS.

Come disattivare la funzione?

Puoi disattivare questa funzione in qualsiasi momento. Se nel sistema sono presenti utenti con restrizioni, è necessario prima ripristinare il loro accesso.

- In Workload Security, vai a **Workload Security > Criteri > Criteri di risposta automatica**. Seleziona **+Politica di attacco**.
- Deseleziona (deseleziona) *Blocca accesso file utente*.

La funzionalità verrà nascosta da tutte le pagine.

Ripristina manualmente gli IP per NFS

Per ripristinare manualmente gli IP da ONTAP se il periodo di prova di Workload Security scade o se l'agente/collettore è inattivo, attenersi alla seguente procedura.

1. Elenca tutte le policy di esportazione su una SVM.

```
contrail-qa-fas8020:> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Eliminare le regole in tutti i criteri sull'SVM che hanno "cloudsecure_rule" come corrispondenza client specificando il rispettivo RuleIndex. La regola di sicurezza del carico di lavoro sarà solitamente impostata su 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Assicurarsi che la regola Workload Security sia stata eliminata
(passaggio facoltativo per la conferma).
```

```
contrail-qa-fas8020:*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Ripristina manualmente gli utenti per SMB

Per ripristinare manualmente gli utenti da ONTAP se il periodo di prova di Workload Security scade o se l'agente/collector è inattivo, procedere come segue.

È possibile ottenere l'elenco degli utenti bloccati in Workload Security dalla pagina dell'elenco degli utenti.

1. Accedi al cluster ONTAP (in cui desideri sbloccare gli utenti) con le credenziali *admin* del cluster. (Per Amazon FSx, accedi con le credenziali FSx).
2. Eseguire il seguente comando per elencare tutti gli utenti bloccati da Workload Security per SMB in tutte le SVM:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

Nell'output sopra riportato, 2 utenti sono stati bloccati (US030, US040) con dominio CSLAB.

1. Una volta identificata la posizione dall'output sopra, eseguiamo il seguente comando per sbloccare l'utente:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Per confermare che gli utenti siano sbloccati, eseguire il comando:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Non devono essere visualizzate voci per gli utenti precedentemente bloccati.

Risoluzione dei problemi

Problema	Prova questo
Alcuni utenti non sono soggetti a restrizioni, nonostante ci sia un attacco.	1. Assicurarsi che il Data Collector e l'agente per le SVM siano nello stato *In esecuzione*. Workload Security non sarà in grado di inviare comandi se Data Collector e Agent sono arrestati. 2. Ciò accade perché l'utente potrebbe aver avuto accesso all'archiviazione da una macchina con un nuovo IP mai utilizzato in precedenza. La limitazione avviene tramite l'indirizzo IP dell'host tramite il quale l'utente accede allo storage. Controllare nell'interfaccia utente (Dettagli avviso > Cronologia limitazioni di accesso per questo utente > IP interessati) l'elenco degli indirizzi IP soggetti a restrizioni. Se l'utente accede allo storage da un host con un IP diverso dagli IP con restrizioni, potrà comunque accedere allo storage tramite l'IP senza restrizioni. Se l'utente tenta di accedere dagli host i cui IP sono limitati, l'archiviazione non sarà accessibile.
Cliccando manualmente su Limita accesso si ottiene il messaggio "Gli indirizzi IP di questo utente sono già stati limitati".	L'IP da limitare è già limitato a un altro utente.
La politica non può essere modificata. Motivo: non autorizzato per quel comando.	Controllare se si utilizza csuser, che le autorizzazioni siano concesse all'utente come indicato sopra.

Problema	Prova questo
Il blocco dell'utente (indirizzo IP) per NFS funziona, ma per SMB/CIFS vedo un messaggio di errore: "La trasformazione da SID a DomainName non è riuscita. Motivo del timeout: il socket non è stato stabilito"	Ciò può accadere se *csuser* non ha l'autorizzazione per eseguire ssh. (Assicurarsi che la connessione sia a livello di cluster, quindi assicurarsi che l'utente possa eseguire ssh). Il ruolo *csuser* richiede queste autorizzazioni. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Per *csuser* con credenziali cluster, procedere come segue dalla riga di comando ONTAP : security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all Se *csuser* non viene utilizzato e se viene utilizzato l'utente amministratore a livello di cluster, assicurarsi che l'utente amministratore disponga dell'autorizzazione SSH per ONTAP.
Ricevo il messaggio di errore *SID translate failed. Reason:255:Error: command failed: not authorized for that commandError: "access-check" is not a recognized command*, quando un utente avrebbe dovuto essere bloccato.	Ciò può accadere quando *csuser* non dispone delle autorizzazioni corrette. Vedere "Prerequisiti per il blocco dell'accesso utente" per maggiori informazioni. Dopo aver applicato le autorizzazioni, si consiglia di riavviare il raccoglitore dati ONTAP e il raccoglitore dati della directory utente. Di seguito sono elencati i comandi di autorizzazione richiesti. ---- creazione ruolo di accesso di sicurezza -role csrole -cmddirname "regola policy di esportazione vserver" -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname set -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname "sessione cifs vserver" -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname "traduzione autenticazione controllo accesso servizi vserver" -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname "mappatura nome vserver" -access all ----

Sicurezza del carico di lavoro: simulazione della manomissione dei file

È possibile utilizzare le istruzioni presenti in questa pagina per simulare la manomissione dei file a scopo di test o dimostrazione della sicurezza del carico di lavoro utilizzando lo script di simulazione della manomissione dei file incluso.

Cose da notare prima di iniziare

- Lo script di simulazione della manomissione dei file funziona solo su Linux. Lo script di simulazione dovrebbe anche generare avvisi di elevata affidabilità nel caso in cui l'utente abbia integrato ONTAP ARP con Workload Security.
- Workload Security rileverà gli eventi e gli avvisi generati con NFS 4.1 solo se la versione ONTAP è 9.15 o successiva.
- Lo script è fornito con i file di installazione dell'agente Workload Security. È disponibile su qualsiasi macchina su cui sia installato un agente Workload Security.
- È possibile eseguire lo script direttamente sulla macchina dell'agente Workload Security; non è necessario preparare un'altra macchina Linux. Tuttavia, se preferisci eseguire lo script su un altro sistema, ti basterà copiarlo ed eseguirlo lì.
- Gli utenti possono scegliere tra Python o script shell in base alle proprie preferenze e ai requisiti di sistema.
- Lo script Python richiede installazioni preliminari. Se non vuoi usare Python, usa lo script shell.

Linee guida:

Questo script dovrebbe essere eseguito su una SVM contenente una cartella con un numero considerevole di file da crittografare, idealmente 100 o più, inclusi i file nelle sottocartelle. Assicurarsi che i file non siano vuoti.

Per generare l'avviso, mettere temporaneamente in pausa il raccoglitore prima di creare i dati di prova. Una volta generati i file di esempio, riavviare il raccoglitore e avviare il processo di crittografia.

Passaggi:

Preparare il sistema:

Per prima cosa, montare il volume di destinazione sulla macchina. È possibile montare un'esportazione NFS o CIFS.

Per montare l'esportazione NFS in Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Non montare NFS versione 4.1; non è supportato da Fpolicy.

Per montare CIFS in Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

Abilita ONTAP Autonomous Ransomware Protection (facoltativo):

Se la versione del cluster ONTAP è 9.11.1 o successiva, è possibile abilitare il servizio ONTAP Ransomware Protection eseguendo il seguente comando sulla console di comando ONTAP .

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
Successivamente, configura un Data Collector:
```

1. Configurare l'agente Workload Security se non è già stato fatto.
2. Se non è già stato fatto, configurare un raccoglitore dati SVM.
3. Assicurarsi che il protocollo di montaggio sia selezionato durante la configurazione del raccoglitore dati.

Generare i file di esempio a livello di programmazione:

Prima di creare i file, è necessario prima arrestare o"mettere in pausa il raccoglitore dati" elaborazione.

Prima di eseguire la simulazione, è necessario aggiungere i file da crittografare. È possibile copiare manualmente i file da crittografare nella cartella di destinazione oppure utilizzare uno degli script inclusi per creare i file in modo programmatico. Qualunque sia il metodo utilizzato, assicurati che siano presenti almeno 100 file da crittografare.

Se si sceglie di creare i file a livello di programmazione, è possibile utilizzare Shell o Python:

Conchiglia:

1. Accedi alla casella Agente.
2. Montare una condivisione NFS o CIFS dall'SVM del filer alla macchina dell'agente. Vai a quella cartella.
3. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh) nella posizione di montaggio di destinazione.
4. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per creare la cartella e i file del set di dati di prova:

```
 './create_dataset.sh'
. Verranno creati 100 file non vuoti con varie estensioni all'interno
della cartella di montaggio, in una directory denominata "test_dataset".
```

Pitone:

Prerequisito per lo script Python:

- Installa Python (se non è già installato).
  - Scarica Python 3.5.2 o versione successiva da https://www.python.org/ .
  - Per verificare l'installazione di Python, eseguire `python --version` .
  - Lo script Python è stato testato a partire dalla versione 3.5.2.
- Installare pip se non è già installato:
  - Scarica lo script get-pip.py da https://bootstrap.pypa.io/ .
  - Installa pip usando `python get-pip.py` .

- Verificare l'installazione del pip con `pip --version` .

- Libreria PyCryptodome:
  - Lo script utilizza la libreria PyCryptodome.
  - Installa PyCryptodome con `pip install pycryptodome` .
  - Confermare l'installazione di PyCryptodome eseguendo `pip show pycryptodome` .

Script di creazione file Python:

1. Accedi alla casella Agente.
2. Montare una condivisione NFS o CIFS dall'SVM del filer alla macchina dell'agente. Vai a quella cartella.
3. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) nella posizione di montaggio di destinazione.
4. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per creare la cartella e i file del set di dati di prova:

```
 'python create_dataset.py'
. Questo creerà 100 file non vuoti con varie estensioni all'interno
della cartella di montaggio sotto una directory chiamata "test_dataset"
```

Riprendi il collezionista

Se hai messo in pausa il raccoglitore prima di seguire questi passaggi, assicurati di riavviarlo una volta creati i file di esempio.

Generare i file di esempio a livello di programmazione:

Prima di creare i file, è necessario prima arrestare o"mettere in pausa il raccoglitore dati" elaborazione.

Per generare un avviso di manomissione di file, è possibile eseguire lo script incluso che simulerà un avviso di manomissione di file in Workload Security.

Conchiglia:

1. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) nella posizione di montaggio di destinazione.
2. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per crittografare il set di dati di prova:

```
 './simulate_attack.sh'
. In questo modo verranno crittografati i file di esempio creati nella
directory "test_dataset".
```

Pitone:

1. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) nella posizione di montaggio di destinazione.
2. Si prega di notare che i prerequisiti Python sono installati come da sezione Prerequisiti dello script Python
3. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per crittografare il set di dati di prova:

```
 'python simulate_attack.py'
. In questo modo verranno crittografati i file di esempio creati nella
directory "test_dataset".
```

Genera un avviso in Workload Security

Una volta terminata l'esecuzione dello script del simulatore, entro pochi minuti verrà visualizzato un avviso sull'interfaccia utente Web.

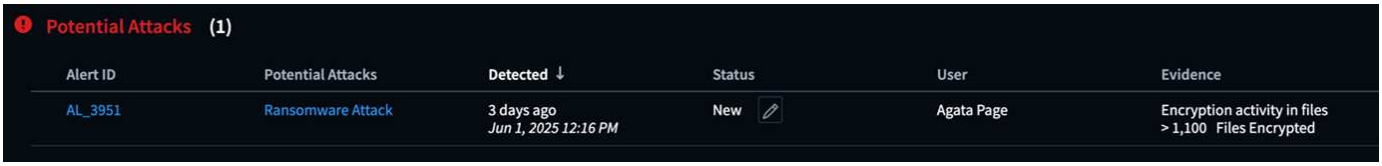
Nota: nel caso in cui siano soddisfatte tutte le seguenti condizioni, verrà generato un avviso di elevata affidabilità.

1. Versione ONTAP di SVM monitorata superiore a 9.11.1
2. Protezione autonoma dal ransomware ONTAP configurata
3. Il raccoglitore di dati di sicurezza del carico di lavoro è stato aggiunto in modalità Cluster.

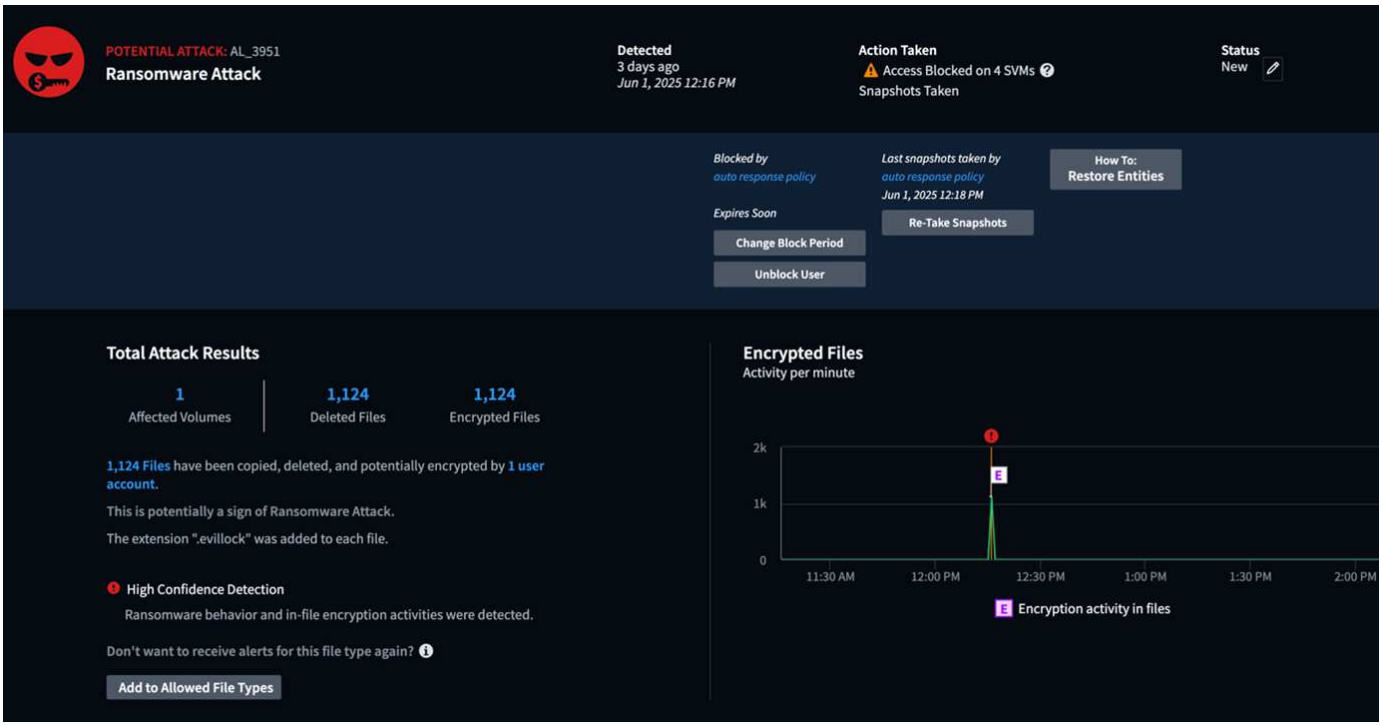
Workload Security rileva i modelli di manomissione dei file in base al comportamento dell'utente, mentre ONTAP ARP rileva le attività di manomissione dei file in base alle attività di crittografia nei file.

Se le condizioni sono soddisfatte, Workload Security contrassegna gli avvisi come avviso di elevata affidabilità.

Esempio di avviso di elevata affidabilità nella pagina dell'elenco degli avvisi:



Esempio di dettaglio dell'avviso di elevata affidabilità:



Attivazione dell'avviso più volte

Workload Security apprende il comportamento dell'utente e non genererà avvisi in caso di ripetuti attacchi di manomissione dei file entro 24 ore per lo stesso utente.

Per generare un nuovo avviso con un utente diverso, ripetere gli stessi passaggi (creazione dei dati di prova e successiva crittografia dei dati di prova).

Configurazione delle notifiche e-mail per avvisi, avvertenze e stato di integrità dell'agente/collettore dell'origine dati

Le notifiche e-mail ti consentono di rimanere informato su potenziali attacchi, avvisi di sicurezza e problemi di integrità dell'infrastruttura non appena si verificano. Configura gli indirizzi email dei destinatari nelle impostazioni Amministrazione > Notifiche per ricevere avvisi in tempo reale personalizzati in base alle responsabilità di ciascun destinatario.

Avvisi e avvisi di potenziali attacchi

Per inviare notifiche di avviso di *Potenziale attacco*, inserisci gli indirizzi email dei destinatari nella sezione *Invia avvisi di potenziale attacco*. Per ogni azione sull'avviso vengono inviate notifiche e-mail all'elenco dei destinatari dell'avviso.

Per inviare notifiche di *Avviso*, inserisci gli indirizzi email dei destinatari nella sezione *Invia avvisi di avviso*.

Monitoraggio dello stato di salute dell'agente e del raccoglitore dati

È possibile monitorare lo stato di salute degli agenti e delle origini dati tramite notifiche.

Per ricevere notifiche nel caso in cui un agente o un raccoglitore di origini dati non funzioni, immettere gli indirizzi e-mail dei destinatari nella sezione *Avvisi sullo stato di integrità della raccolta dati*.

Tieni presente quanto segue:

- Gli avvisi sanitari verranno inviati solo dopo che l'agente/esattore avrà smesso di segnalare per almeno un'ora.
- Viene inviata una sola notifica e-mail ai destinatari previsti in un dato periodo di 24 ore, anche se l'agente o il raccoglitore dati sono disconnessi per un periodo di tempo più lungo.
- In caso di errore dell'agente, verrà inviato un avviso (non uno per ogni collettore). L'e-mail conterrà un elenco di tutti gli SVM interessati.
- L'errore di raccolta di Active Directory viene segnalato come avviso; non influisce sul rilevamento delle minacce.
- L'elenco di configurazione introduttiva ora include una nuova fase *Configura notifiche e-mail*.

Ricezione di notifiche di aggiornamento dell'agente e del raccoglitore dati

- Inserire l'ID e-mail in "Avvisi sanitari sulla raccolta dati".
- La casella di controllo "Abilita notifiche di aggiornamento" diventa abilitata.
- Le notifiche e-mail relative all'aggiornamento di Agent e Data Collector vengono inviate agli ID e-mail un giorno prima dell'aggiornamento pianificato.

Risoluzione dei problemi

Problema:	Prova questo:
Gli ID e-mail sono presenti negli "Avvisi sullo stato di salute del Data Collector", tuttavia non ricevo notifiche.	Le email di notifica vengono inviate dal dominio NetApp Data Infrastructure Insights , ovvero da *accounts@service.cloudinsights.netapp.com*. Alcune aziende bloccano le email in arrivo se provengono da un dominio esterno. Assicurarsi che le notifiche esterne provenienti dai domini NetApp Data Infrastructure Insights siano inserite nella whitelist.

Notifiche webhook

Notifiche di sicurezza del carico di lavoro tramite webhook

I webhook consentono agli utenti di inviare notifiche di avviso critiche o di avvertimento a varie applicazioni utilizzando un canale webhook personalizzato.

Molte applicazioni commerciali supportano i webhook come interfaccia di input standard, ad esempio: Slack, PagerDuty, Teams e Discord. Supportando un canale webhook generico e personalizzabile, Workload Security può supportare molti di questi canali di distribuzione. Le informazioni sulla configurazione dei webhook sono disponibili sui siti web delle rispettive applicazioni. Ad esempio, Slack fornisce"questa guida utile" .

È possibile creare più canali webhook, ognuno dei quali è destinato a uno scopo diverso, ad applicazioni separate, a destinatari diversi, ecc.

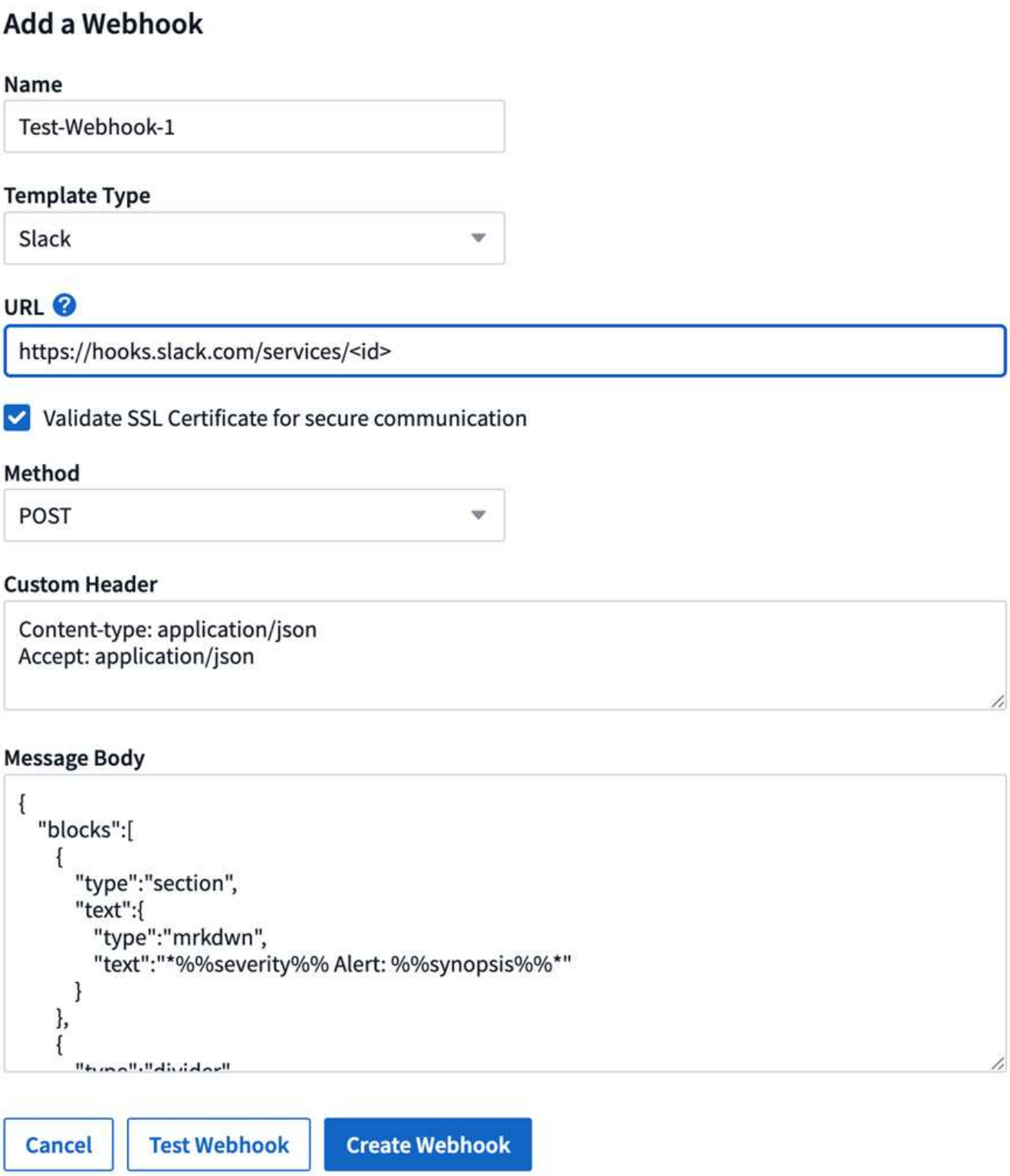
L'istanza del canale webhook è composta dai seguenti elementi

Nome	Descrizione
URL	URL di destinazione del webhook, incluso il prefisso http:// o https:// insieme ai parametri URL
Metodo	GET/POST - Il valore predefinito è POST
Intestazione personalizzata	Specifica qui eventuali intestazioni personalizzate
Corpo del messaggio	Inserisci qui il corpo del tuo messaggio
Parametri di avviso predefiniti	Elenca i parametri predefiniti per il webhook
Parametri e segreti personalizzati	I parametri e i segreti personalizzati consentono di aggiungere parametri univoci ed elementi sicuri come le password

Creazione di un webhook

Per creare un webhook di sicurezza del carico di lavoro, vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". L'immagine seguente mostra un esempio di schermata di creazione di un webhook Slack.

Nota: per creare e gestire i webhook di Workload Security, l'utente deve essere un amministratore di Workload Security.



- Inserisci le informazioni appropriate per ciascun campo e fai clic su "Salva".
- Puoi anche cliccare sul pulsante "Test Webhook" per testare la connessione. Si noti che in questo modo verrà inviato il "Corpo del messaggio" (senza sostituzioni) all'URL definito in base al metodo selezionato.
- I webhook SWS comprendono una serie di parametri predefiniti. Inoltre, puoi creare parametri o segreti personalizzati.

Parametri: cosa sono e come utilizzarli?

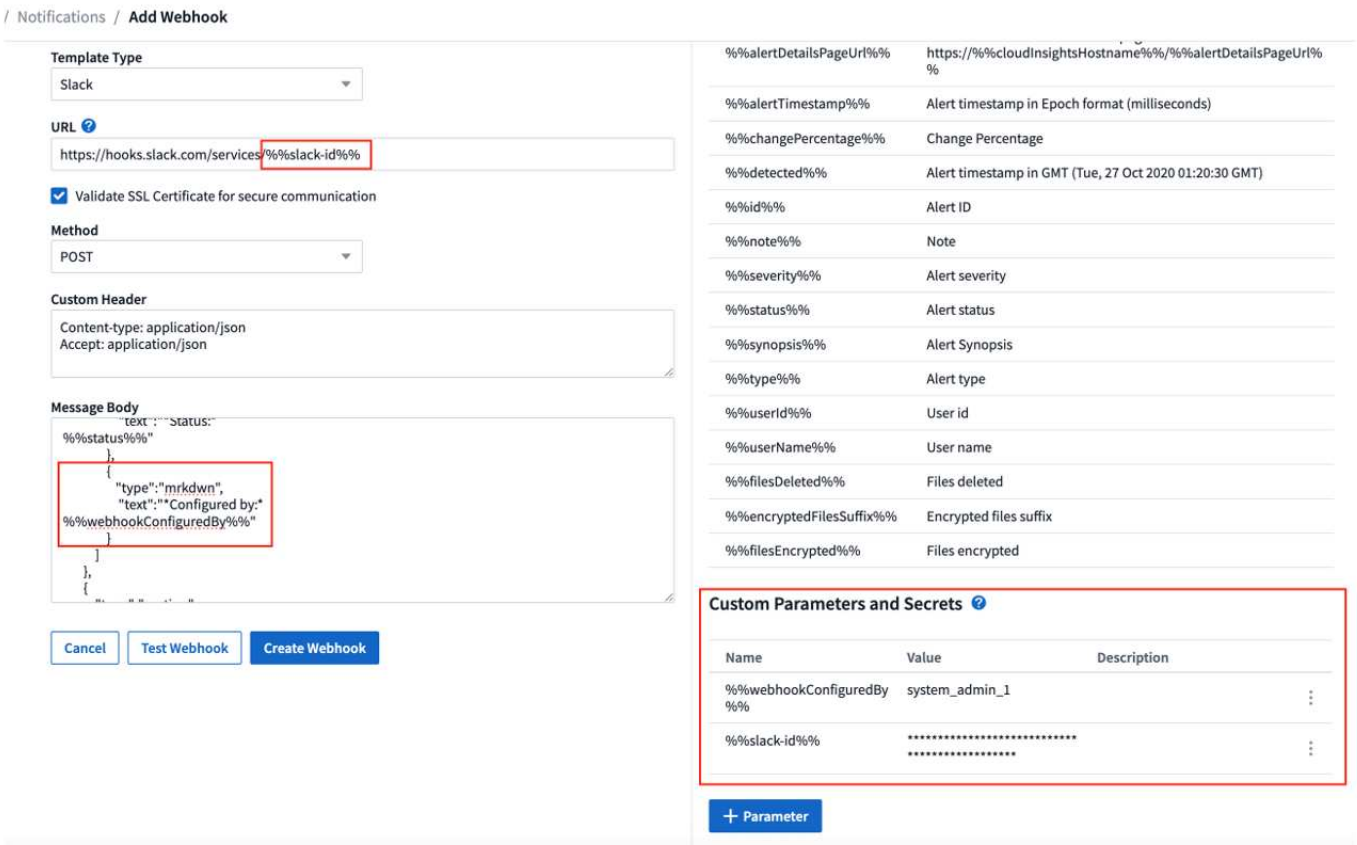
I parametri di avviso sono valori dinamici popolati per avviso. Ad esempio, il parametro *%%severity%%* verrà sostituito con il tipo di gravità dell'avviso.

Si noti che le sostituzioni non vengono eseguite quando si fa clic sul pulsante "Test Webhook"; il test invia un payload che mostra i segnaposto del parametro (*%%<param-name>%%*) ma non li sostituisce con i dati.

Parametri e segreti personalizzati

In questa sezione puoi aggiungere tutti i parametri personalizzati e/o segreti che desideri. Un parametro personalizzato o un segreto può essere presente nell'URL o nel corpo del messaggio. I segreti consentono all'utente di configurare un parametro personalizzato sicuro come password, apiKey ecc.

L'immagine di esempio seguente mostra come vengono utilizzati i parametri personalizzati nella creazione di webhook.



Pagina elenco webhook sicurezza carico di lavoro

Nella pagina dell'elenco dei webhook vengono visualizzati i campi Nome, Creato da, Creato il, Stato, Sicuro e Ultimo segnalato. Nota: il valore della colonna "stato" continuerà a cambiare in base al risultato dell'ultimo trigger del webhook. Di seguito sono riportati alcuni esempi di risultati di stato.

Stato	Descrizione
OK	Notifica inviata correttamente.
403	Vietato.
404	URL non trovato.

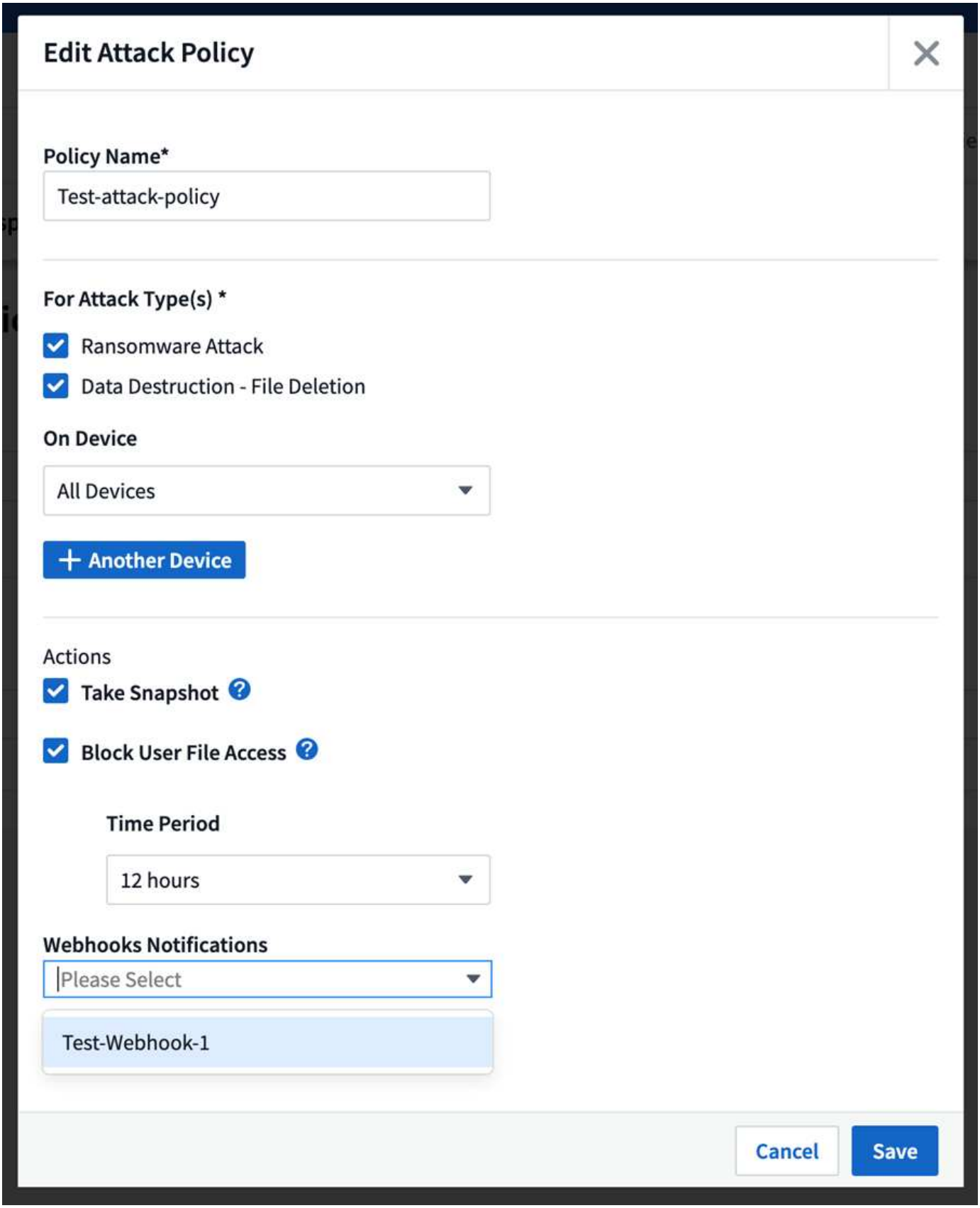
400	Brutta richiesta. Potresti visualizzare questo stato se c'è un errore nel corpo del messaggio, ad esempio: • JSON formattato male. • Fornito valore non valido per le chiavi riservate. Ad esempio, PagerDuty accetta solo informazioni critiche/avviso/errore/informazioni per "Gravità". Qualsiasi altro risultato potrebbe comportare lo stato 400. • Errori di convalida specifici dell'applicazione. Ad esempio, Slack consente un massimo di 10 campi all'interno di una sezione. Includerne più di 10 può comportare lo stato 400.
410	La risorsa non è più disponibile

La colonna "Ultimo segnalato" indica l'ora in cui il webhook è stato attivato l'ultima volta.

Dalla pagina dell'elenco dei webhook gli utenti possono anche modificare/duplicare/eliminare i webhook.

Configurare la notifica Webhook nel criterio di avviso

Per aggiungere una notifica webhook a un criterio di avviso, vai su -Sicurezza del carico di lavoro > Criteri- e seleziona un criterio esistente o aggiungine uno nuovo. Nella sezione *Azioni* > menu a discesa *Notifiche webhook*, seleziona i webhook richiesti.



Le notifiche webhook sono collegate alle policy. Quando si verifica l'attacco (RW/DD/WARN), verrà eseguita l'azione configurata (Scatta snapshot/blocco utente) e verrà quindi attivata la notifica webhook associata.

Nota: le notifiche e-mail sono indipendenti dalle policy e verranno attivate come di consueto.

- Se una policy viene sospesa, le notifiche webhook non verranno attivate.
- È possibile associare più webhook a una singola policy, ma si consiglia di non associarne più di 5.

Esempi di webhook sulla sicurezza del carico di lavoro

Webhook per"Slack"

Webhook per"PagerDuty" Webhook per"Squadre" Webhook per"Discordia"

Esempio di webhook di sicurezza del carico di lavoro per Discord

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Discord.

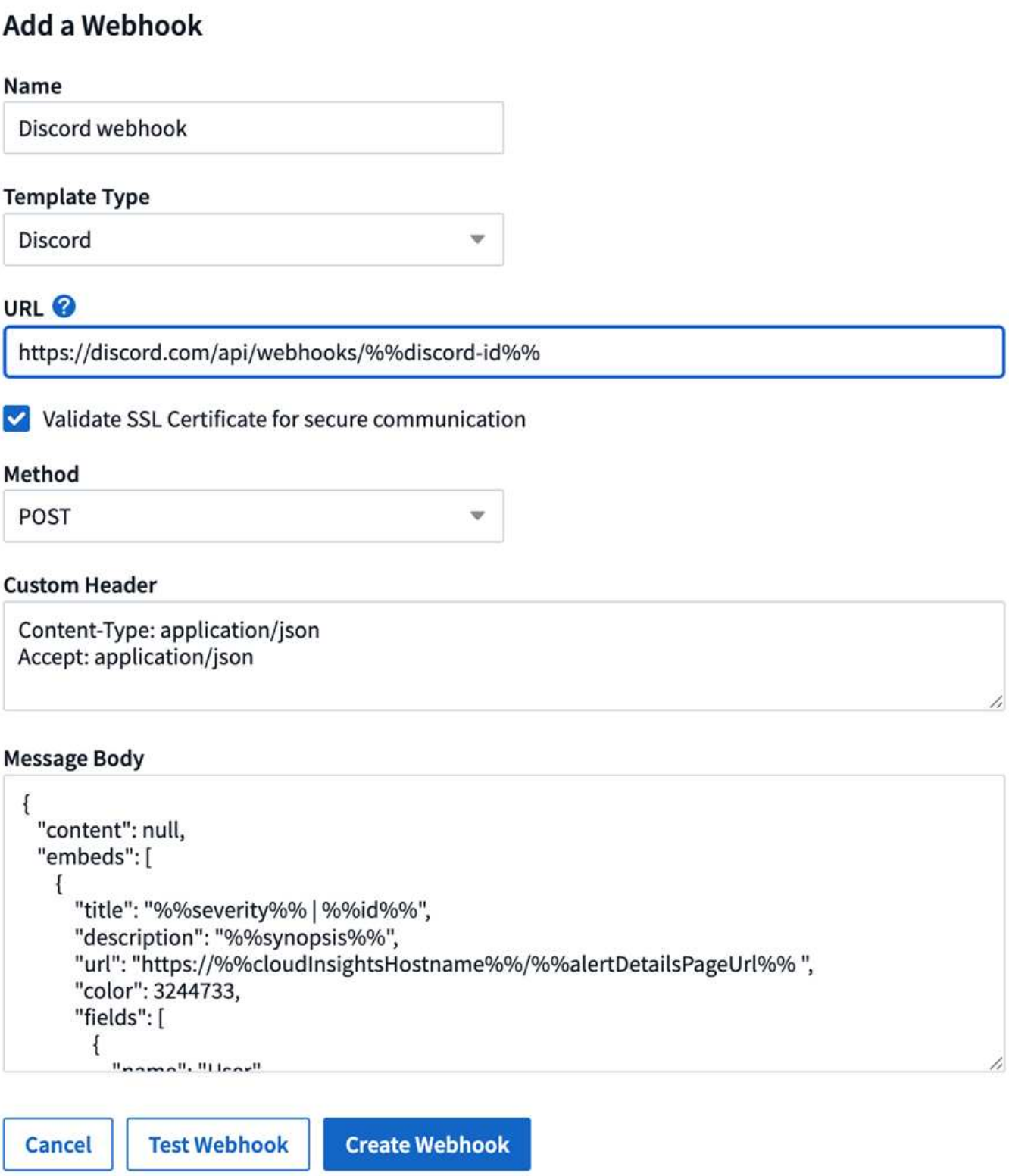
Questa pagina fa riferimento a istruzioni di terze parti, che sono soggette a modifiche. Fare riferimento al"Documentazione Discord" per le informazioni più aggiornate.

Configurazione Discord:

- In Discord, seleziona il server, in Canali di testo, seleziona Modifica canale (icona a forma di ingranaggio)
- Seleziona **Integrazioni > Visualizza webhook** e fai clic su **Nuovo webhook**
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook sulla sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Fare clic su '+ Webhook' per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Discord**.
4. Incolla l'URL di Discord riportato sopra nel campo *URL*.



Per testare il webhook, sostituisci temporaneamente il valore URL nel corpo del messaggio con un URL valido (ad esempio *https://netapp.com*), quindi fai clic sul pulsante *Test Webhook*. Per far funzionare la funzionalità Test Webhook, Discord richiede che venga fornito un URL valido.

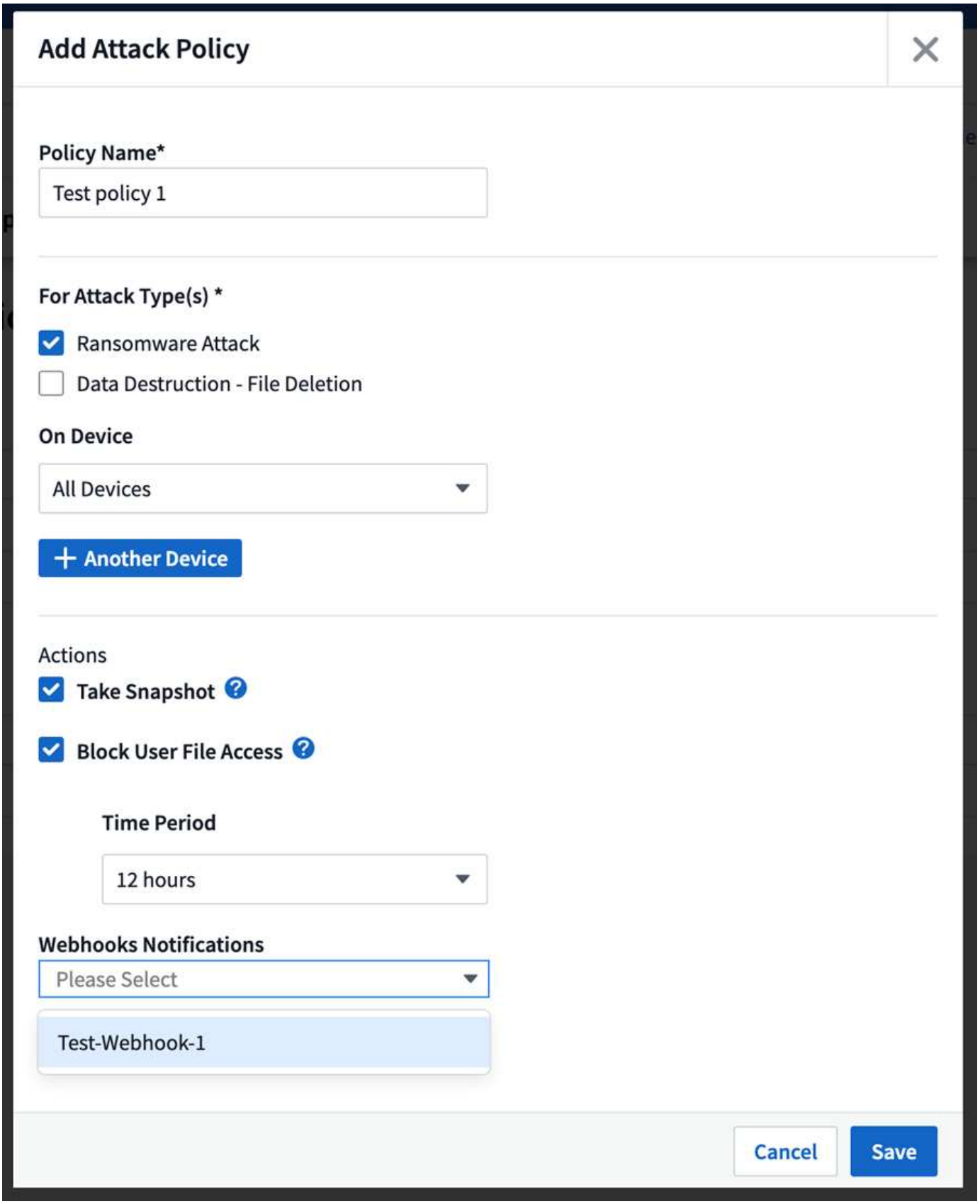
Una volta completato il test, assicurati di reimpostare il corpo del messaggio.

Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui associare la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook Discord desiderati e salva.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



Esempio di webhook di sicurezza del carico di lavoro per PagerDuty

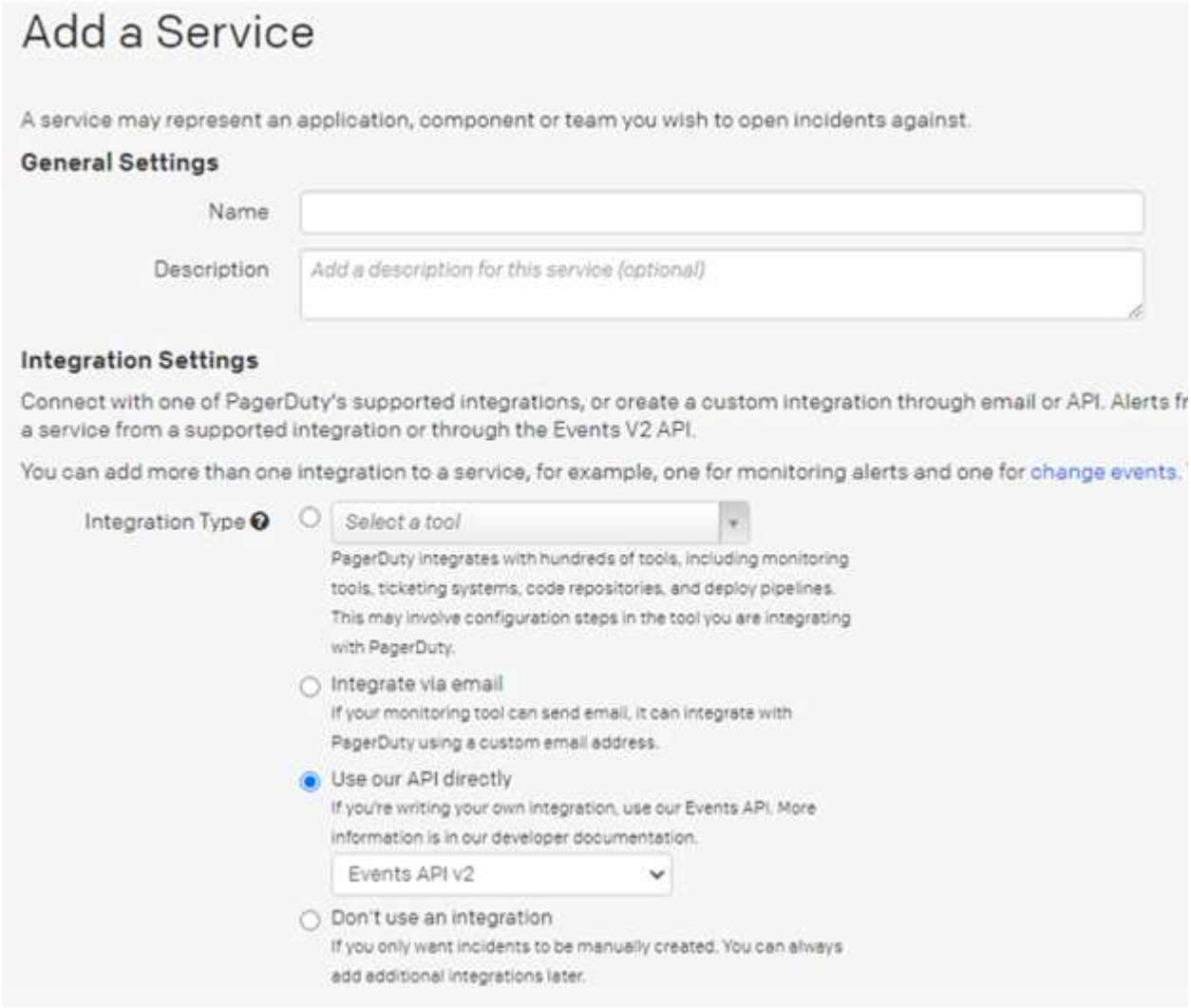
I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per

impostare webhook per PagerDuty.

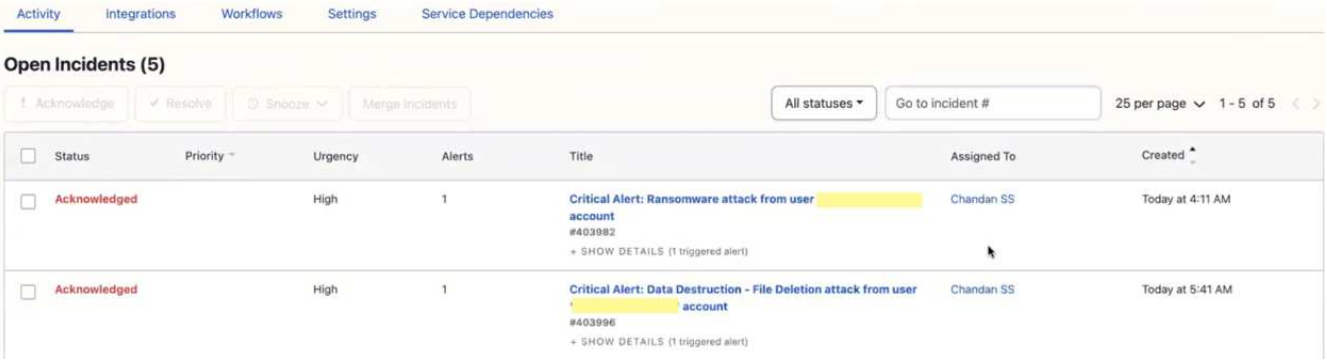
Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento al"Documentazione PagerDuty" per le informazioni più aggiornate.

Configurazione PagerDuty:

1. In PagerDuty, vai su **Servizi > Directory dei servizi** e clicca sul pulsante **+Nuovo servizio**.
2. Inserisci un *Nome* e seleziona *Usa direttamente la nostra API*. Selezionare *Aggiungi servizio*.

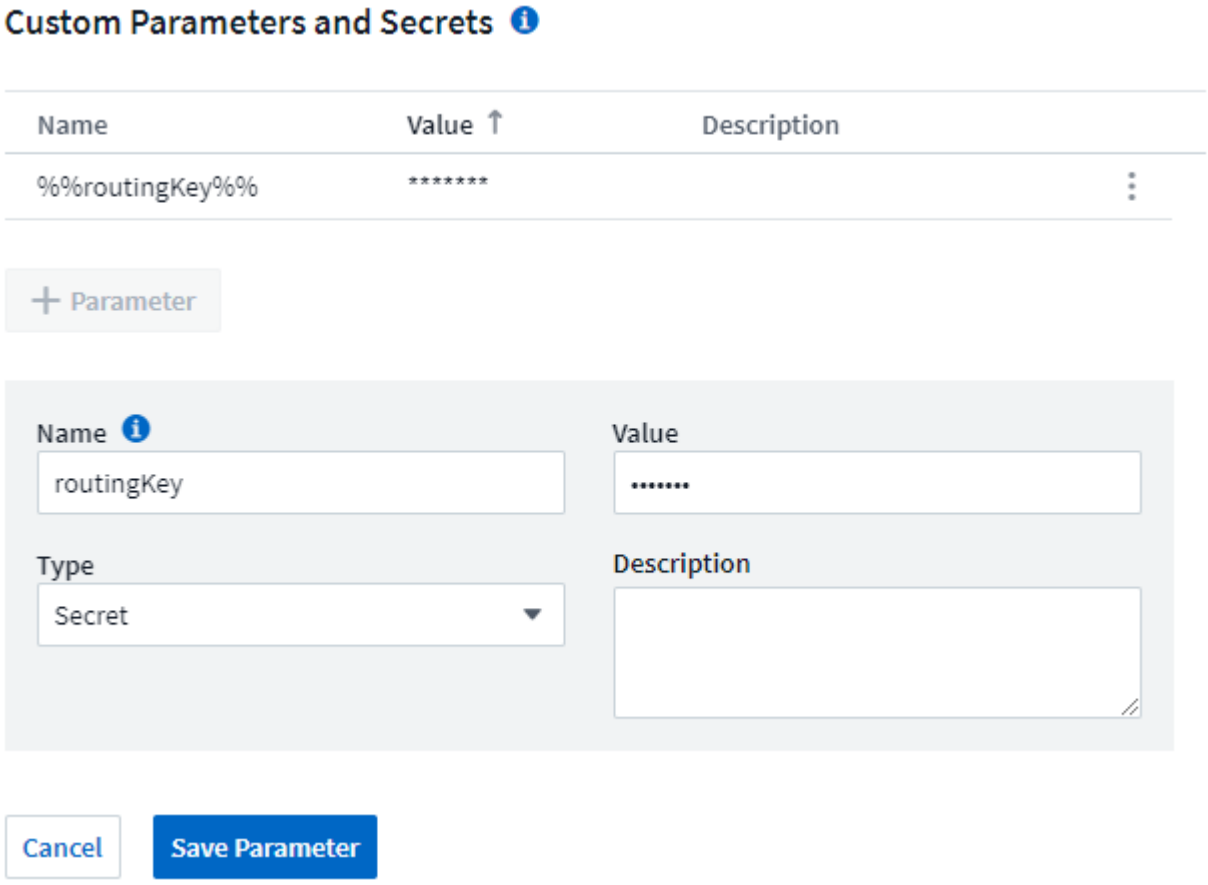


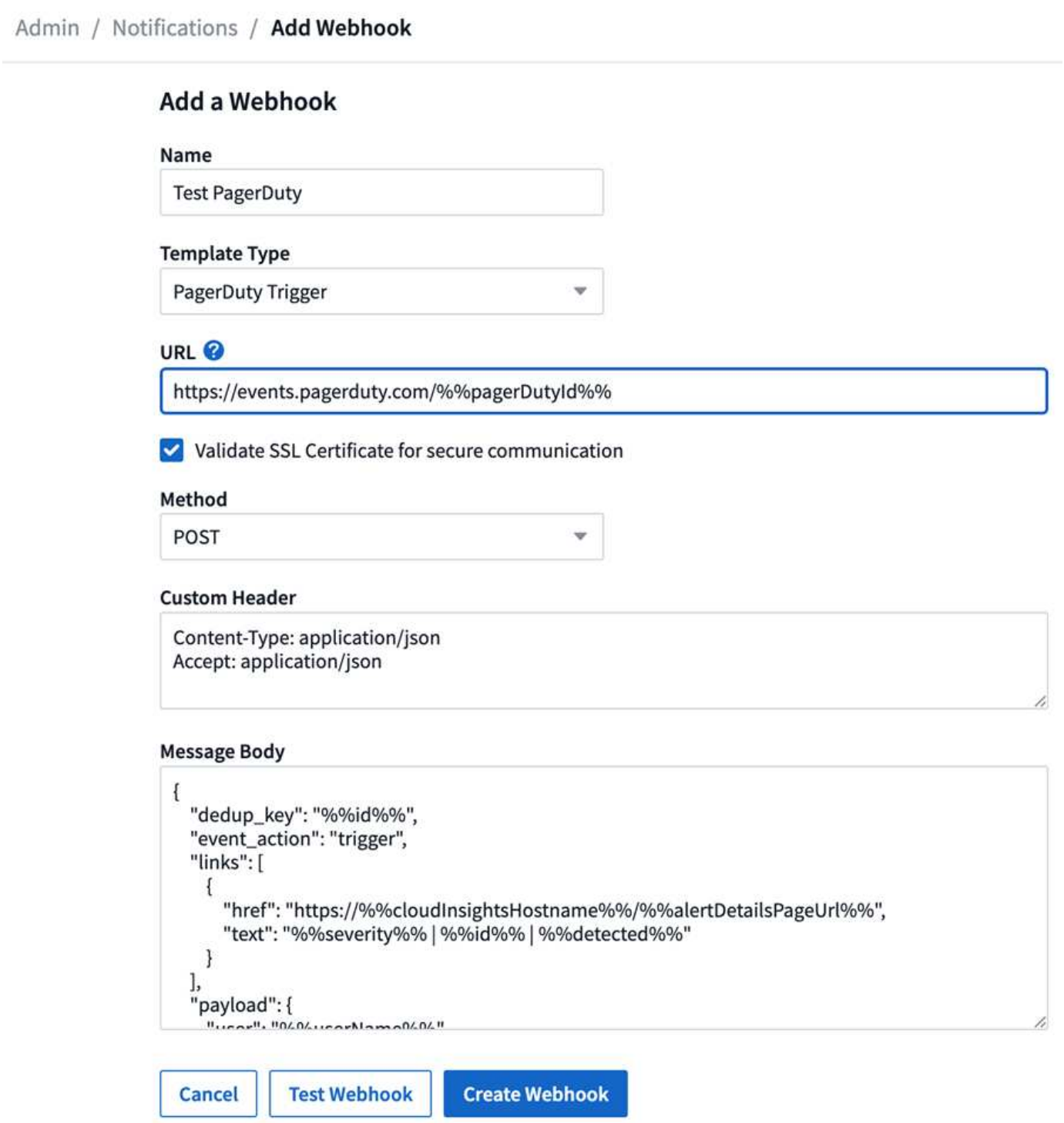
3. Selezionare la scheda *Integrazioni* per visualizzare la **Chiave di integrazione**. Questa chiave ti servirà quando creerai il webhook Workload Security qui sotto.
4. Vai a **Incidenti** o **Servizi** per visualizzare gli avvisi.



Crea webhook Workload Security PagerDuty:

- Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare '+ Webhook' per creare un nuovo webhook.
- Assegnare al webhook un nome significativo.
- Nel menu a discesa *Tipo di modello*, seleziona *Trigger PagerDuty*.
- Crea un parametro segreto personalizzato denominato *routingKey* e imposta il valore sulla *Chiave di integrazione* PagerDuty creata in precedenza.

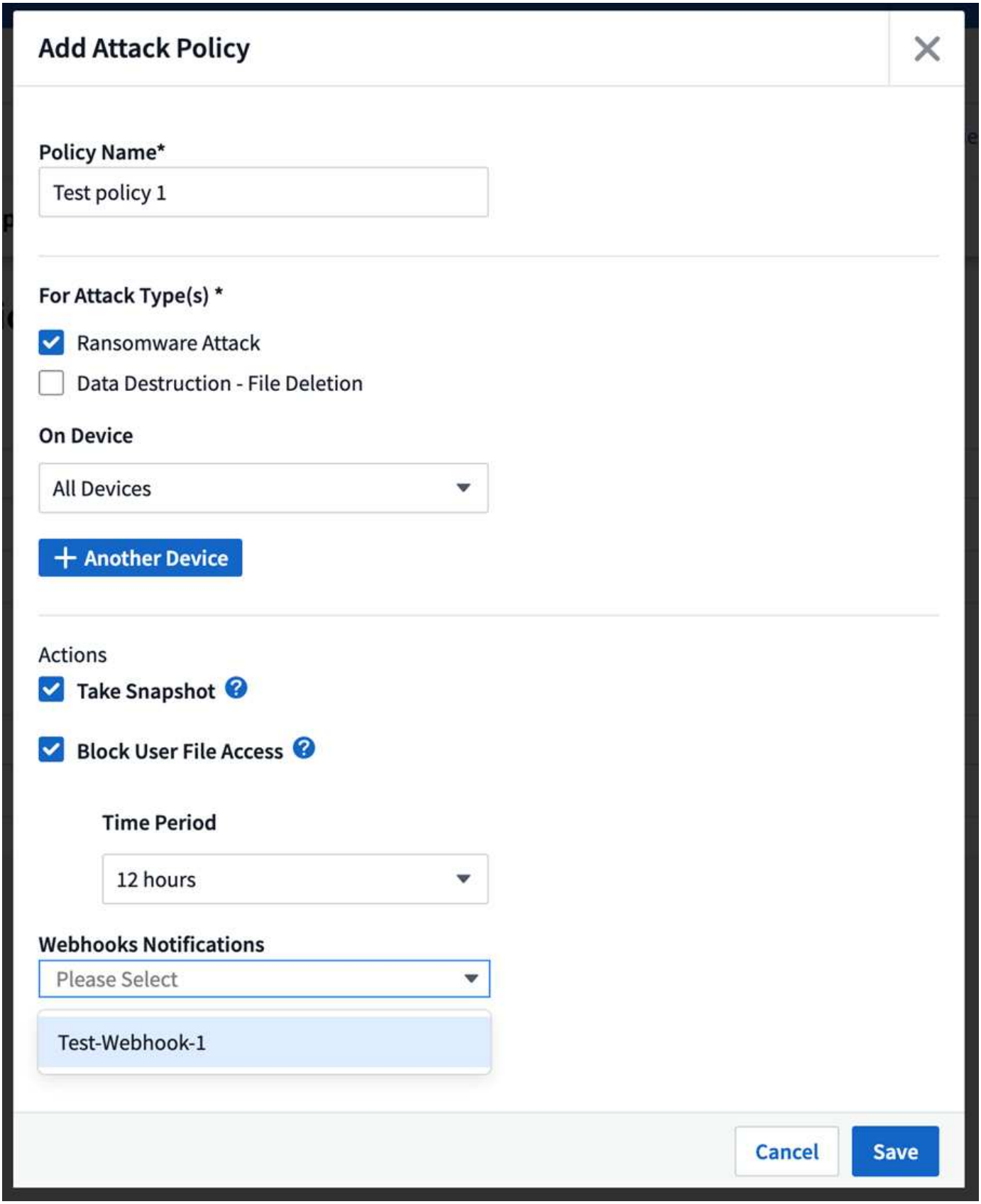




Notifiche tramite Webhook

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro > Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook PagerDuty desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



Esempio di webhook di sicurezza del carico di lavoro per Slack

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni

utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Slack.

Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Per informazioni più aggiornate, consultare la documentazione di Slack.

Esempio di Slack

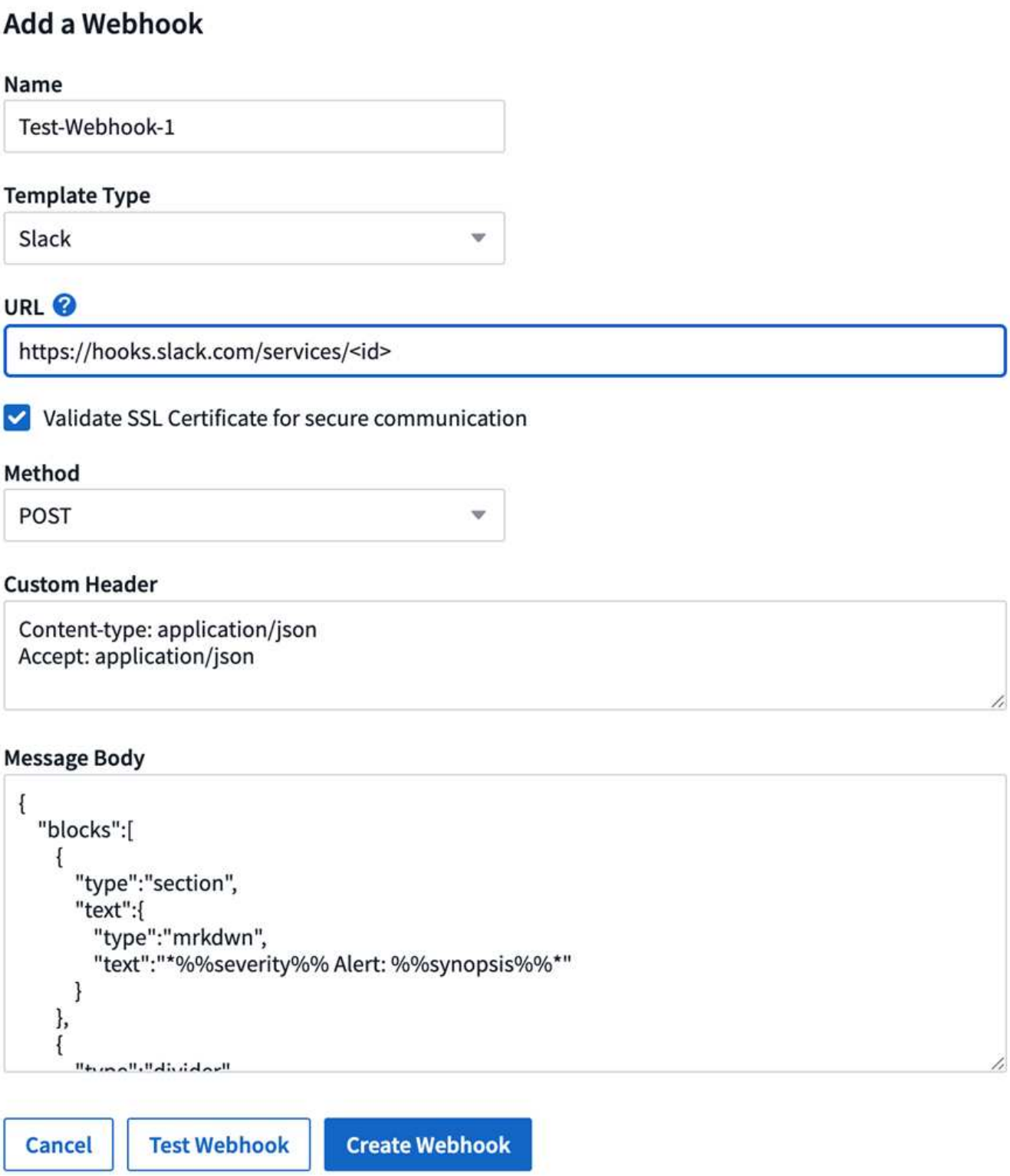
- Vai a https://api.slack.com/apps e crea una nuova app. Assegnagli un nome significativo e seleziona un'area di lavoro.

- Vai a Webhook in arrivo, clicca su *Attiva webhook in arrivo*, seleziona *Aggiungi nuovo webhook* e seleziona il canale su cui pubblicare.
- Copia l'URL del webhook. Questo URL verrà fornito durante la creazione di un webhook di Workload

Security.

Crea un webhook Slack per la sicurezza del carico di lavoro

1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona *Slack*.
4. Incolla l'URL copiato sopra.

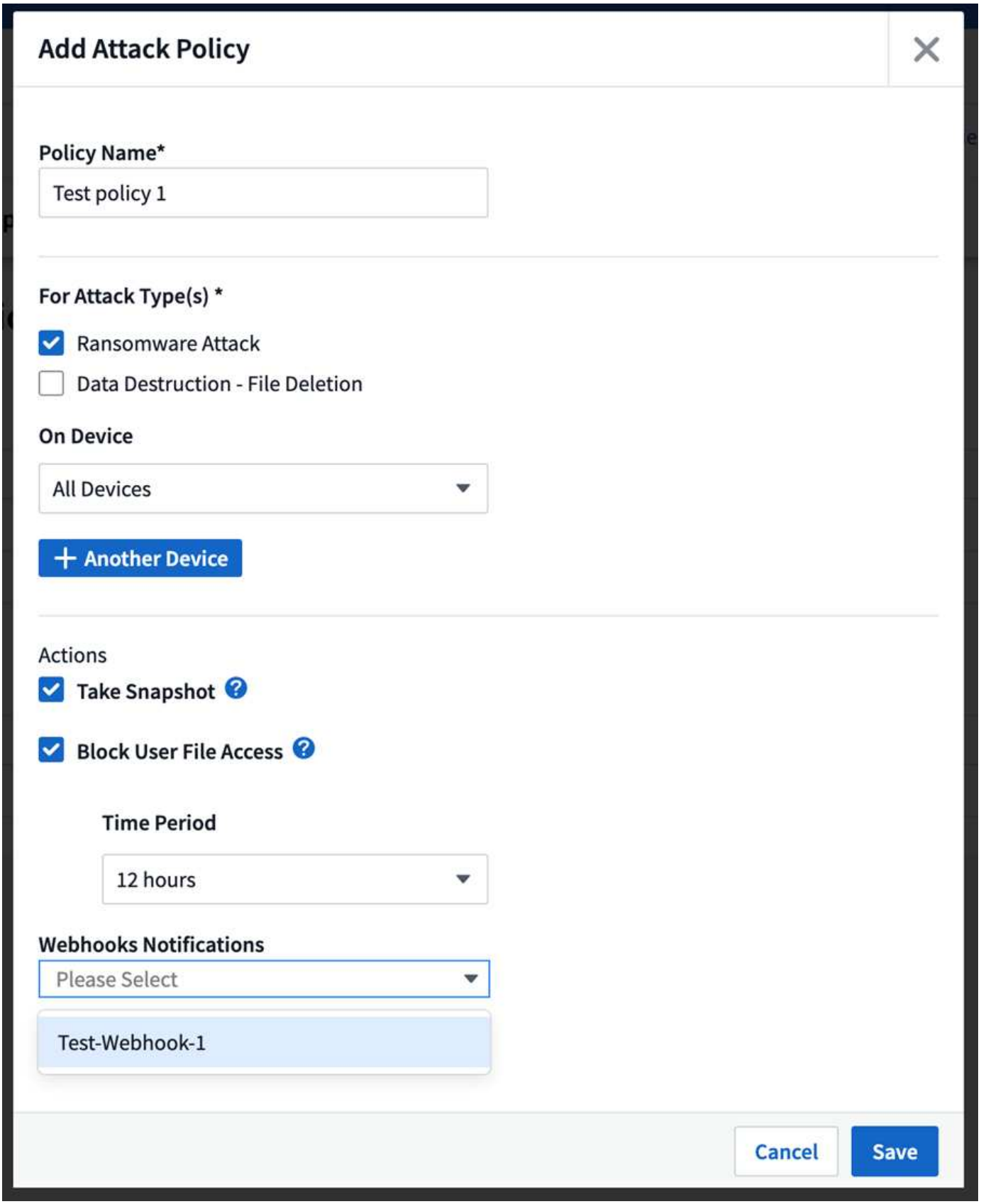


Notifiche tramite webhook

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.

- Nel menu a discesa *Notifiche webhook*, seleziona i webhook desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



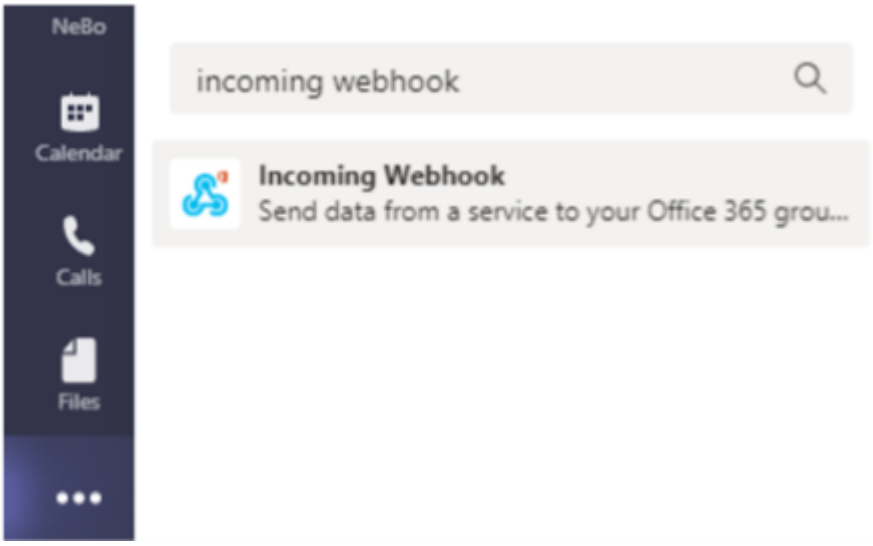
Esempio di webhook di sicurezza del carico di lavoro per Microsoft Teams

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per la configurazione di webhook per Teams.

Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento al"Documentazione dei team" per le informazioni più aggiornate.

Configurazione delle squadre:

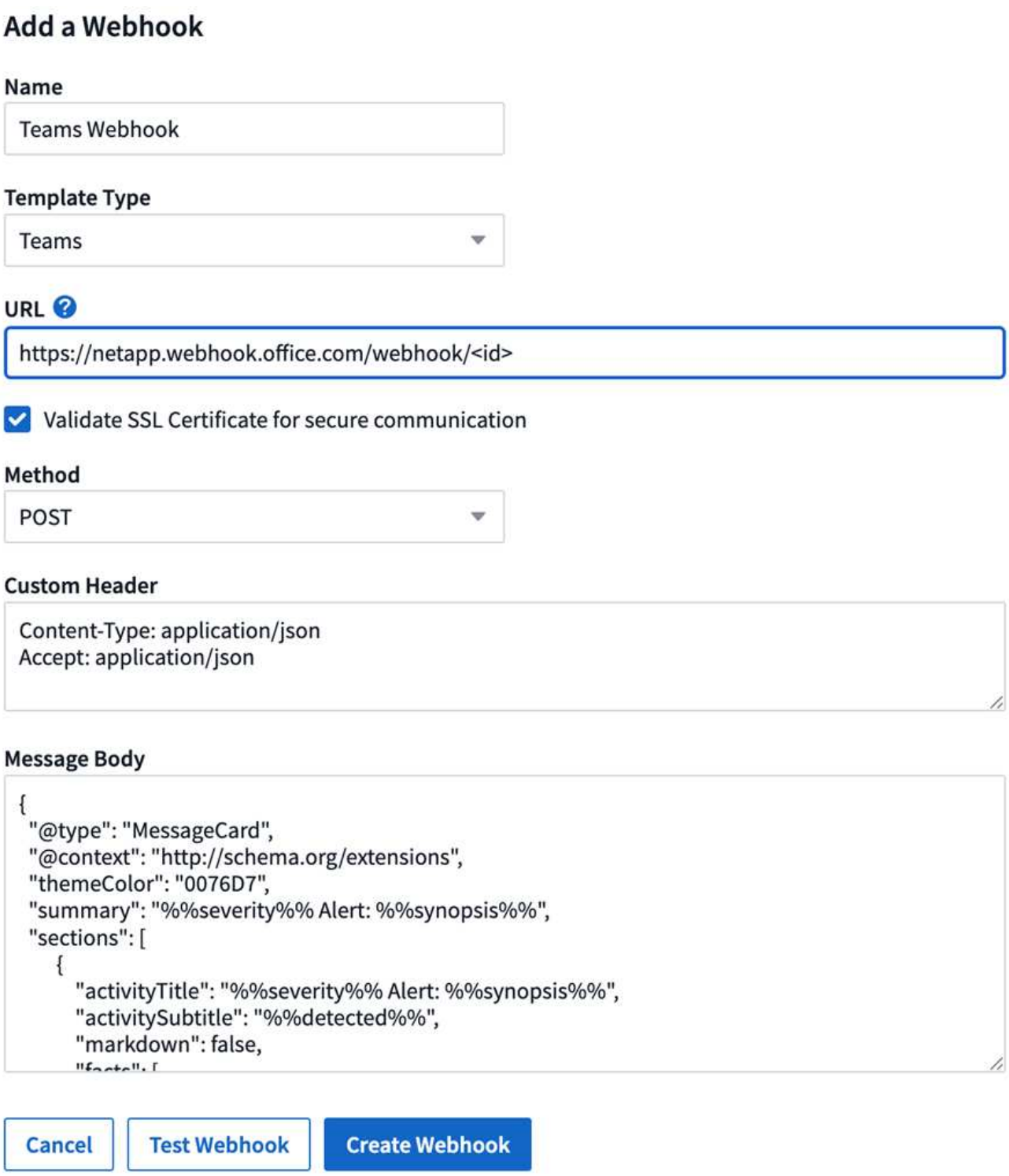
1. In Teams, seleziona il kebab e cerca Webhook in arrivo.



2. Seleziona **Aggiungi a un team > Seleziona un team > Imposta un connettore**.
3. Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook per i team di sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Team**.



4. Incolla l'URL sopra nel campo *URL*.

Passaggi per creare notifiche Teams con il modello Adaptive Card

1. Sostituisci il corpo del messaggio con il seguente template:

```
{
"type": "message",
"attachments": [
```

```
{
  "contentType": "application/vnd.microsoft.card.adaptive",
  "content": {
    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
    "type": "AdaptiveCard",
    "version": "1.2",
    "body": [
      {
        "type": "TextBlock",
        "text": "%%severity%% Alert: %%synopsis%%",
        "wrap": true,
        "weight": "Bolder",
        "size": "Large"
      },
      {
        "type": "TextBlock",
        "text": "%%detected%%",
        "wrap": true,
        "isSubtle": true,
        "spacing": "Small"
      },
      {
        "type": "FactSet",
        "facts": [
          {
            "title": "User",
            "value": "%%userName%%"
          },
          {
            "title": "Attack/Abnormal Behavior",
            "value": "%%type%%"
          },
          {
            "title": "Action taken",
            "value": "%%actionTaken%%"
          },
          {
            "title": "Files encrypted",
            "value": "%%filesEncrypted%%"
          },
          {
            "title": "Encrypted files suffix",
            "value": "%%encryptedFilesSuffix%%"
          },
          {
            "title": "Files deleted",
```

```
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Se si utilizzano i flussi di Power Automate, i parametri di query nell'URL sono in formato codificato. È necessario decodificare l'URL prima di inserirlo.
3. Fare clic su "Test Webhook" per assicurarsi che non vi siano errori.
4. Salva il webhook.

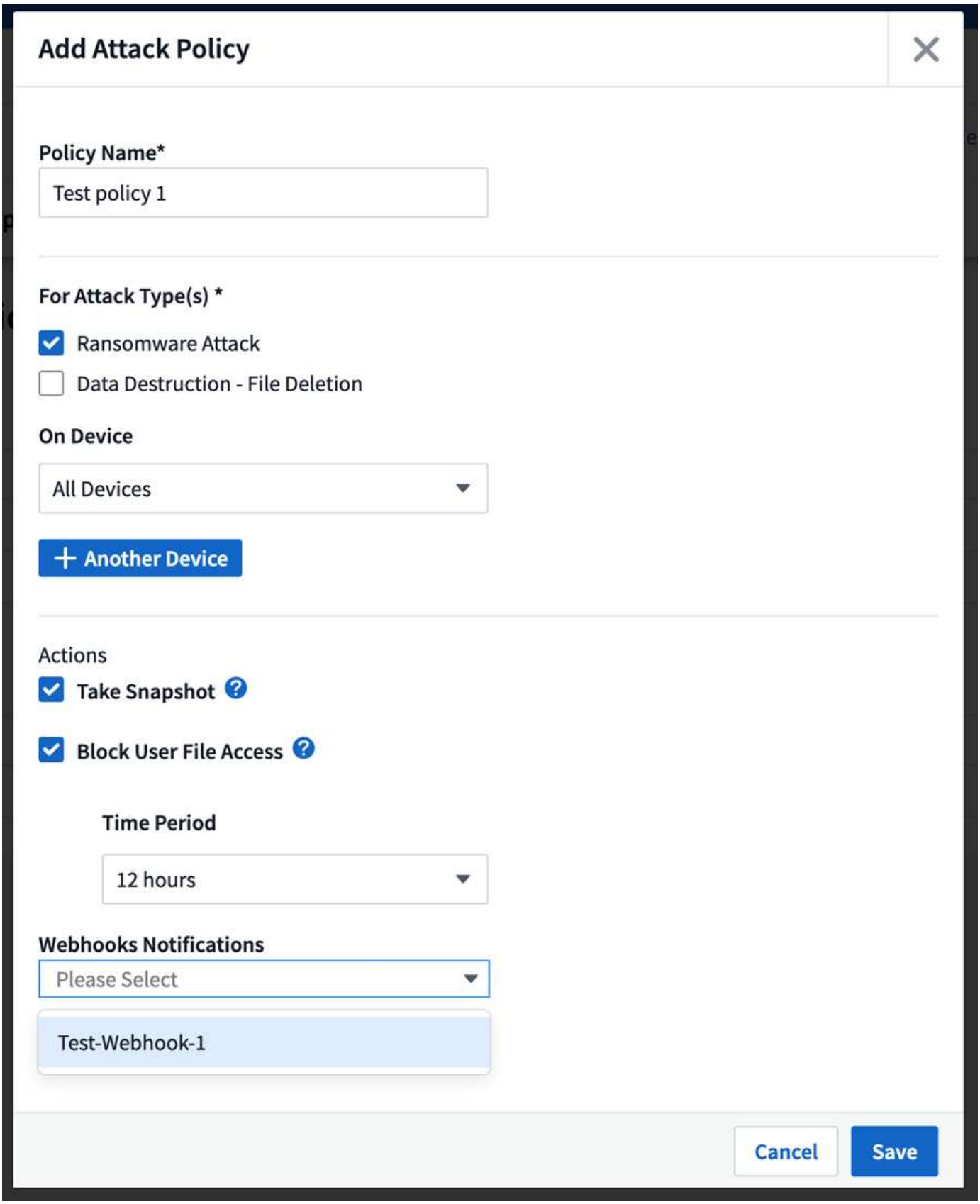
Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.

- Nel menu a discesa *Notifiche webhook*, seleziona i webhook di Teams desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



API di sicurezza del carico di lavoro

Integra Workload Security con il tuo ecosistema aziendale utilizzando un'API REST protetta da un'autenticazione sicura basata su token. Recupera dati di attività forensi, gestisci i token di accesso alle API e sviluppa integrazioni personalizzate con CMDB, sistemi di ticketing e altre applicazioni. La documentazione interattiva Swagger fornisce specifiche API complete e consente di testare direttamente gli endpoint.

Requisiti per l'accesso all'API:

- Per concedere l'accesso viene utilizzato un modello di token di accesso API.
- La gestione dei token API viene eseguita dagli utenti di Workload Security con il ruolo di amministratore.

Documentazione API (Swagger)

Per reperire le informazioni API più recenti, accedere a Workload Security e andare su **Amministrazione > Accesso API**. Fare clic sul collegamento **Documentazione API**. La documentazione API è basata su Swagger, che fornisce una breve descrizione e informazioni sull'utilizzo dell'API e consente di provarla sul proprio tenant.

Se si richiama l'API Forensics Activity, utilizzare l'API cloudsecure_forensics.activities.**v2**. Se si effettuano più chiamate a questa API, assicurarsi che le chiamate avvengano in sequenza e non in parallelo. Più chiamate parallele potrebbero causare il timeout dell'API.

Token di accesso API

Prima di utilizzare l'API Workload Security, è necessario creare uno o più **token di accesso API**. I token di accesso concedono permessi di lettura. È anche possibile impostare la scadenza per ciascun token di accesso.

Per creare un token di accesso:

- Fare clic su **Amministrazione > Accesso API**
- Fai clic su **+Token di accesso API**
- Inserisci **Nome token**
- Specifica **Scadenza token**

Il tuo token potrà essere copiato negli appunti e salvato solo durante il processo di creazione. Una volta creati, i token non possono essere recuperati, pertanto si consiglia vivamente di copiarli e salvarli in un luogo sicuro. Ti verrà chiesto di fare clic sul pulsante Copia token di accesso API prima di poter chiudere la schermata di creazione del token.

È possibile disattivare, attivare e revocare i token. I token disabilitati possono essere abilitati.

I token garantiscono l'accesso generico alle API dal punto di vista del cliente, gestendo l'accesso alle API nell'ambito del proprio tenant.

L'applicazione riceve un token di accesso dopo che un utente si è autenticato e ha autorizzato l'accesso, quindi passa il token di accesso come credenziale quando chiama l'API di destinazione. Il token trasmesso informa l'API che il portatore del token è stato autorizzato ad accedere all'API ed eseguire azioni specifiche in

base all'ambito concesso durante l'autorizzazione.

L'intestazione HTTP in cui viene passato il token di accesso è **X-CloudInsights-ApiKey:**

Ad esempio, utilizzare quanto segue per recuperare le risorse di archiviazione:

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
Dove _<API_Access_Token>_ è il token salvato durante la creazione della
chiave di accesso API e _<Workload Security Tenant>_ è l'URL del tenant
del tuo ambiente Workload Security.
```

Informazioni dettagliate sono disponibili nel link *Documentazione API* in **Amministrazione > Accesso API**.

Script per estrarre dati tramite API

Gli agenti Workload Security includono uno script di esportazione per facilitare le chiamate parallele all'API v2 suddividendo l'intervallo di tempo richiesto in batch più piccoli.

Lo script si trova in */opt/netapp/cloudsecure/agent/export-script*. Un file README nella stessa directory fornisce le istruzioni per l'uso.

Ecco un comando di esempio per richiamare lo script:

```
python3 data-export.py --tenant_url <Workload Security tenant>
--access_key %ACCESS_KEY% --path_filter "<dir path>" --user_name "<user>"
--from_time "01-08-2024 00:00:00" --to_time "31-08-2024 23:59:59"
--iteration_interval 12 --num_workers 3
```

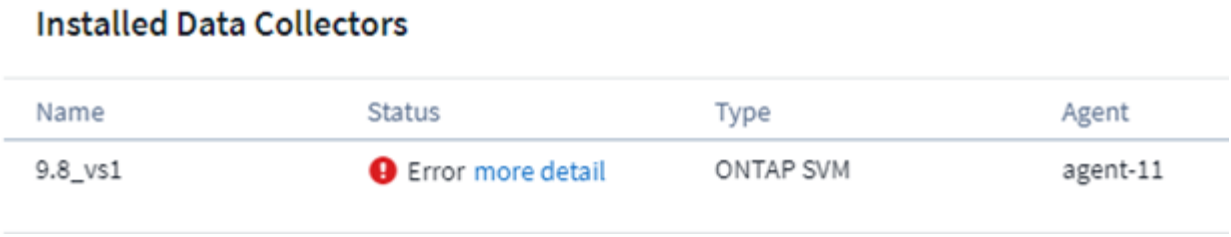
Parametri chiave: - `--iteration_interval 12` : Suddivide l'intervallo di tempo richiesto in intervalli di 12 ore. - `--num_workers 3` : Recupera questi intervalli in parallelo utilizzando 3 thread.

Risoluzione dei problemi del raccoglitore dati ONTAP SVM

Workload Security utilizza dei collettori di dati per raccogliere dati sui file e sugli accessi degli utenti dai dispositivi. Qui puoi trovare suggerimenti per la risoluzione dei problemi relativi a questo raccoglitore.

Vedi il"Configurazione del collettore SVM" pagina per le istruzioni sulla configurazione di questo raccoglitore.

In caso di errore, è possibile fare clic su *ulteriori dettagli* nella colonna *Stato* della pagina Collettori dati installati per ottenere maggiori dettagli sull'errore.



Di seguito vengono descritti i problemi noti e le relative soluzioni.

Problema: Data Collector funziona per un po' di tempo e si arresta dopo un tempo casuale, con il seguente messaggio di errore: "Messaggio di errore: il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno sovraccarico." **Prova questo:** la frequenza degli eventi di ONTAP era molto più alta di quella che la casella Agent può gestire. Di conseguenza la connessione è stata interrotta.

Controlla il picco di traffico in CloudSecure al momento della disconnessione. Puoi verificarlo dalla pagina **CloudSecure > Activity Forensics > Tutte le attività**.

Se il traffico aggregato di picco è superiore a quello che l'Agent Box può gestire, fare riferimento alla pagina Event Rate Checker per informazioni su come dimensionare la distribuzione del Collector in un Agent Box.

Se l'agente è stato installato nella casella Agente prima del 4 marzo 2021, eseguire i seguenti comandi nella casella Agente:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Dopo il ridimensionamento, riavviare il raccoglitore dall'interfaccia utente.

{vuoto}

Problema: il Collector segnala il messaggio di errore: "Nessun indirizzo IP locale trovato sul connettore in grado di raggiungere le interfacce dati dell'SVM". **Prova questo:** Molto probabilmente è dovuto a un problema di rete sul lato ONTAP . Si prega di seguire questi passaggi:

1. Assicurarsi che non vi siano firewall sulla vita dati SVM o sulla vita di gestione che bloccano la connessione dalla SVM.
2. Quando si aggiunge una SVM tramite un IP di gestione del cluster, assicurarsi che la vita dati e la vita di gestione della SVM siano pingabili dalla VM dell'agente. In caso di problemi, controllare il gateway, la netmask e i percorsi per lif.

   Puoi anche provare ad accedere al cluster tramite ssh utilizzando l'IP di gestione del cluster ed effettuare il ping dell'IP dell'agente. Assicurarsi che l'IP dell'agente sia pingabile:

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

3. Se hai provato a connetterti tramite l'IP del cluster e non funziona, prova a connetterti direttamente tramite l'IP SVM. Per i passaggi necessari per connettersi tramite IP SVM, vedere quanto sopra.
4. Durante l'aggiunta del collettore tramite IP SVM e credenziali vsadmin, verificare se SVM Lif ha abilitato il ruolo Data plus Mgmt. In questo caso il ping all'SVM Lif funzionerà, ma l'SSH all'SVM Lif non funzionerà. In caso affermativo, creare un SVM Mgmt Only Lif e provare a connettersi tramite questo SVM Management Only Lif.
5. Se ancora non funziona, crea un nuovo SVM Lif e prova a connetterti tramite quel Lif. Assicurarsi che la subnet mask sia impostata correttamente.
6. Debug avanzato:
   a. Avvia una traccia dei pacchetti in ONTAP.
   b. Provare a connettere un data collector all'SVM dall'interfaccia utente di CloudSecure.
   c. Attendi finché non compare l'errore. Arresta la traccia dei pacchetti in ONTAP.
   d. Aprire la traccia del pacchetto da ONTAP. È disponibile in questa posizione

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Assicurarsi che ci sia un SYN da ONTAP alla casella Agent.
.. Se non c'è SYN da ONTAP , allora c'è un problema con il firewall
in ONTAP.
.. Aprire il firewall in ONTAP, in modo che ONTAP possa connettersi
alla casella agente.
```

7. Se il problema persiste, consultare il team di rete per accertarsi che nessun firewall esterno stia bloccando la connessione da ONTAP alla casella Agent.
8. Se nessuna delle soluzioni precedenti risolve il problema, apri un caso con"Supporto Netapp" per ulteriore assistenza.

{vuoto}

Problema: Messaggio: "Impossibile determinare il tipo ONTAP per [nome host: <indirizzo IP>. Motivo: Errore di connessione al sistema di archiviazione <Indirizzo IP>: Host non raggiungibile (Host non raggiungibile)
Prova questo:

1. Verificare che sia stato fornito l'indirizzo IP di gestione SVM o l'IP di gestione del cluster corretto.
2. Eseguire l'SSH sull'SVM o sul Cluster a cui si intende connettersi. Una volta effettuata la connessione, assicurarsi che il nome SVM o Cluster sia corretto.

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno terminato." **Prova questo:**

1. È molto probabile che un firewall stia bloccando le porte necessarie nella macchina dell'agente. Verificare che l'intervallo di porte 35000-55000/tcp sia aperto affinché la macchina agente possa connettersi dall'SVM. Assicurarsi inoltre che non vi siano firewall abilitati sul lato ONTAP che bloccano la comunicazione con la macchina agente.
2. Digitare il seguente comando nella casella Agente e assicurarsi che l'intervallo di porte sia aperto.

   ```
   sudo iptables-save | grep 3500*
   ```

   L'output di esempio dovrebbe apparire così:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Accedi a SVM, inserisci i seguenti comandi e verifica che non sia
   impostato alcun firewall per bloccare la comunicazione con ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Controlla i comandi del firewall"sul lato ONTAP .

3. Accedi tramite SSH all'SVM/Cluster che vuoi monitorare. Eseguire il ping della casella Agent dalla libreria dati SVM (con supporto dei protocolli CIFS e NFS) e assicurarsi che il ping funzioni:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

4. Se un singolo SVM viene aggiunto due volte a un tenant tramite 2 collettori dati, verrà visualizzato questo errore. Eliminare uno dei collettori di dati tramite l'interfaccia utente. Quindi riavviare l'altro raccoglitore dati tramite l'interfaccia utente. Quindi il raccoglitore dati mostrerà lo stato "IN ESECUZIONE" e inizierà a ricevere eventi da SVM.

   In pratica, in un tenant, 1 SVM dovrebbe essere aggiunto una sola volta, tramite 1 data collector. 1 SVM non dovrebbe essere aggiunto due volte tramite 2 collettori di dati.

5. Nei casi in cui lo stesso SVM è stato aggiunto in due diversi ambienti Workload Security (tenant), l'ultimo riuscirà sempre. Il secondo collettore configurerà fpolicy con il proprio indirizzo IP ed espellerà il primo. Quindi il collettore nel primo smetterà di ricevere eventi e il suo servizio di "audit" entrerà in stato di errore. Per evitare ciò, configurare ogni SVM su un singolo ambiente.
6. Questo errore può verificarsi anche se i criteri di servizio non sono configurati correttamente. Con ONTAP 9.8 o versioni successive, per connettersi al Data Source Collector, è necessario il servizio data-fpolicy-

client insieme al servizio dati data-nfs e/o data-cifs. Inoltre, il servizio data-fpolicy-client deve essere associato ai dati lif per l'SVM monitorato.

{vuoto}

Problema: Nessun evento visualizzato nella pagina delle attività. **Prova questo:**

1. Verificare se il collettore ONTAP è nello stato "IN ESECUZIONE". In caso affermativo, assicurarsi che alcuni eventi cifs vengano generati sulle VM client cifs aprendo alcuni file.
2. Se non vengono rilevate attività, effettuare l'accesso all'SVM e immettere il seguente comando.

   ```
   <SVM>event log show -source fpolicy
   ```

   Assicurati che non ci siano errori relativi a fpolicy.

3. Se non vengono visualizzate attività, effettuare l'accesso all'SVM. Immettere il seguente comando:

   ```
   <SVM>fpolicy show
   ```

   Verificare se la policy fpolicy denominata con prefisso "cloudsecure_" è stata impostata e lo stato è "on". Se non è impostato, molto probabilmente l'agente non è in grado di eseguire i comandi nell'SVM. Si prega di assicurarsi che siano stati rispettati tutti i prerequisiti descritti all'inizio della pagina.

{vuoto}

Problema: SVM Data Collector è in stato di errore e il messaggio di errore è "L'agente non è riuscito a connettersi al raccoglitore". **Prova questo:**

1. Molto probabilmente l'agente è sovraccarico e non riesce a connettersi ai collettori dell'origine dati.
2. Controllare quanti collettori di origini dati sono connessi all'agente.
3. Controllare anche la velocità del flusso di dati nella pagina "Tutte le attività" nell'interfaccia utente.
4. Se il numero di attività al secondo è significativamente elevato, installare un altro agente e spostare alcuni dei Data Source Collector sul nuovo agente.

{vuoto}

Problema: SVM Data Collector mostra il messaggio di errore "fpolicy.server.connectError: il nodo non è riuscito a stabilire una connessione con il server FPolicy "12.195.15.146" (motivo: "Selezione scaduta")" **Prova questo:** il firewall è abilitato in SVM/Cluster. Quindi il motore fpolicy non è in grado di connettersi al server fpolicy. Le CLI in ONTAP che possono essere utilizzate per ottenere maggiori informazioni sono:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Controlla i comandi del firewall"sul lato ONTAP .

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Nessuna interfaccia dati valida (ruolo: dati, protocolli dati: NFS o CIFS o entrambi, stato: attivo) trovata sull'SVM." **Prova questo:** assicurati che ci sia un'interfaccia operativa (che abbia il ruolo di dati e protocollo dati come CIFS/NFS).

{vuoto}

Problema: il raccoglitore dati entra nello stato di errore e poi, dopo un po' di tempo, passa allo stato di esecuzione, per poi tornare nuovamente allo stato di errore. Questo ciclo si ripete. **Prova questo:** Questo accade in genere nel seguente scenario:

1. Sono stati aggiunti più raccoglitori di dati.
2. Ai collettori di dati che mostrano questo tipo di comportamento verrà aggiunto 1 SVM. Ciò significa che 2 o più collettori di dati sono collegati a 1 SVM.
3. Assicurarsi che 1 raccoglitore dati si connetta a 1 solo SVM.
4. Eliminare gli altri raccoglitori di dati connessi allo stesso SVM.

{vuoto}

Problema: Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare (policy su SVM svmname. Motivo: Valore non valido specificato per l'elemento 'shares-to-include' in 'fpolicy.policy.scope-modify: "Federal' **Prova questo:** *I nomi delle condivisioni devono essere specificati senza virgolette. Modificare la configurazione DSC ONTAP SVM per correggere i nomi delle condivisioni.

Includi ed escludi azioni non è pensato per un lungo elenco di nomi di azioni. Se hai un gran numero di azioni da includere o escludere, utilizza il filtro per volume.

{vuoto}

Problema: Nel cluster sono presenti fpolicies esistenti che non sono utilizzati. Cosa si dovrebbe fare prima di installare Workload Security? **Prova questo:** Si consiglia di eliminare tutte le impostazioni fpolicy esistenti e non utilizzate, anche se sono in stato disconnesso. Workload Security creerà fpolicy con il prefisso "cloudsecure_". Tutte le altre configurazioni fpolicy non utilizzate possono essere eliminate.

Comando CLI per visualizzare l'elenco fpolicy:

```
 fpolicy show
Passaggi per eliminare le configurazioni fpolicy:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vuoto}

Problema: Dopo aver abilitato Workload Security, le prestazioni ONTAP risultano compromesse: la latenza diventa sporadicamente elevata, mentre gli IOPS diventano sporadicamente bassi. **Prova questo:** Durante l'utilizzo di ONTAP con Workload Security, a volte si possono verificare problemi di latenza in ONTAP. Le possibili cause di ciò sono molteplici, come indicato di seguito:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tutti questi problemi sono stati risolti in ONTAP 9.13.1 e versioni successive; si consiglia vivamente di utilizzare una di queste versioni successive.

{vuoto}

Problema: Data Collector mostra il messaggio di errore: "Errore: impossibile determinare lo stato del collector entro 2 tentativi, provare a riavviare nuovamente il collector (codice errore: AGENT008)". **Prova questo:**

1. Nella pagina dei raccoglitori di dati, scorrere verso destra del raccoglitore di dati che ha generato l'errore e fare clic sul menu con i 3 puntini. Selezionare *Modifica*. Inserire nuovamente la password del raccoglitore dati. Salvare il raccoglitore dati premendo il pulsante *Salva*. Data Collector verrà riavviato e l'errore dovrebbe essere risolto.
2. La macchina dell'agente potrebbe non avere abbastanza CPU o RAM, ecco perché i DSC non funzionano. Controllare il numero di Data Collector aggiunti all'agente nella macchina. Se è superiore a 20, aumentare la capacità della CPU e della RAM della macchina agente. Una volta aumentata la CPU e la RAM, i DSC entreranno automaticamente nello stato di inizializzazione e poi in quello di esecuzione. Consulta la guida alle taglie su"questa pagina" .

{vuoto}

Problema: il Data Collector genera un errore quando è selezionata la modalità SVM. **Prova questo:** durante la connessione in modalità SVM, se per la connessione viene utilizzato l'IP di gestione del cluster anziché l'IP di gestione SVM, la connessione genererà un errore. Assicurarsi che venga utilizzato l'IP SVM corretto.

{vuoto}

Problema: Il raccoglitore dati mostra un messaggio di errore quando la funzione Accesso negato è abilitata: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: impossibile configurare fpolicy su SVM test_svm. Motivo: L'utente non è autorizzato." **Prova questo:** L'utente potrebbe non disporre delle autorizzazioni REST necessarie per la funzionalità Accesso negato. Si prega di seguire le istruzioni su"questa pagina" per impostare i permessi.

Una volta impostate le autorizzazioni, riavviare il raccoglitore.

{vuoto}

Problema: Il collettore è in stato di errore con il messaggio: Il connettore è in stato di errore. Motivo dell'errore: impossibile configurare l'archivio persistente su SVM <Nome SVM>. Motivo: impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova il comando. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare l'archivio persistente su SVM <SVM Name>. Motivo: Impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova a eseguire il comando.

Prova questo: attendi qualche minuto e poi riavvia il Collector.

{vuoto}

Se riscontri ancora problemi, contatta l'assistenza tramite i link indicati nella pagina **Aiuto > Assistenza**.

Risoluzione dei problemi

Risoluzione dei problemi generali Data Infrastructure Insights

Qui troverai suggerimenti per la risoluzione dei problemi Data Infrastructure Insights.

Vedi anche"Risoluzione dei problemi dell'unità di acquisizione Linux" E"Risoluzione dei problemi dell'unità di acquisizione di Windows" .

Problemi di accesso

Problema:	Prova questo:
Data Infrastructure Insights si disconnette automaticamente ogni 6 ore	Ciò è dovuto alla disattivazione dei cookie di terze parti nel browser. Gli utenti possono configurare il proprio browser per abilitare tutti i cookie di terze parti oppure utilizzare un elenco di eccezioni più ristretto per abilitare solo quelli per Data Infrastructure Insights. Esempio: Apri le impostazioni del tuo browser Seleziona l'opzione "Consenti tutti i cookie". **OPPURE** Seleziona "Blocca cookie di terze parti" e aggiungi eccezioni per *[*.]auth0.com* e *[*.]netapp.com*. Microsoft Edge segue lo stesso formato di Chrome per le eccezioni. In Firefox, le eccezioni dei cookie sono semplicemente designate come *auth0.com* e *netapp.com*.
Ho un account Console ma non riesco ad accedere.	Apri un ticket da https://mysupport.netapp.com/site/help . Selezionare la categoria console.netapp.com > Problemi di account/accesso" o console.netapp.com > Problemi di federazione". Sono specificamente per problemi o domande sulla Console. Per tutti gli altri problemi di supporto tecnico Data Infrastructure Insights , contattare"Supporto NetApp" .
Sono stato invitato a Data Infrastructure Insights ma ricevo un messaggio di "non autorizzato".	Verifica di aver creato un account Console o che la tua organizzazione utilizzi l'accesso SSO con Console. Verifica che l'indirizzo email del tuo profilo Console corrisponda all'indirizzo email mostrato nell'email di benvenuto Data Infrastructure Insights . Se l'indirizzo email non corrisponde, richiedi un nuovo invito con l'indirizzo email corretto.
Ho effettuato la disconnessione dalla Console e sono stato automaticamente disconnesso da Data Infrastructure Insights.	Single Sign-On (SSO) su NetApp Cloud Services disconnette tutte le sessioni Data Infrastructure Insights . Se hai accesso a più account Data Infrastructure Insights , la disconnessione da uno qualsiasi di essi comporta la disconnessione di tutte le sessioni attive. Accedi nuovamente per accedere al tuo account.

Problema:	Prova questo:
Dopo diversi giorni sono stato disconnesso automaticamente.	Gli account NetApp Cloud richiedono una nuova autenticazione ogni pochi giorni (l'impostazione attuale della Console è 7 giorni). Accedi nuovamente per accedere al tuo account.
Ricevo un messaggio di errore "non sono più autorizzato ad accedere".	Contatta l'amministratore del tuo account per verificare l'accesso a Data Infrastructure Insights. Verifica che l'indirizzo email del tuo profilo Console corrisponda all'indirizzo email mostrato nell'email di benvenuto Data Infrastructure Insights
Altri errori di accesso	Prova la modalità di navigazione in incognito su Chrome oppure cancella la cronologia, i cookie e la cache del browser. Prova con un profilo browser diverso (ad esempio Chrome - aggiungi Persona).

Altri problemi

Domanda:	Risposta:
Le mie quote rigide Qtree vengono visualizzate correttamente nelle query, ma le mie quote flessibili vengono visualizzate come capacità totale del volume. È corretto?	Verranno visualizzate come quote impostate solo le quote rigide, impostate manualmente o tramite Trident; se non vengono specificate quote rigide, la capacità di Qtree sarà la capacità del volume interno.
Ho impostato manualmente sia una quota flessibile che una quota rigida nello stesso Qtree, ma la capacità totale visualizzata è la quota rigida; è corretto?	Sì, se viene specificata una quota fissa, questa verrà mostrata come capacità totale.
Quando inserisco un orario di pianificazione per un report Cognos, a volte mi ritrovo con una "m" in più nell'orario di pianificazione. Ad esempio, se inserisco l'ora come "02:15 PM", potrebbe essere aggiunto un carattere extra: "02:15 PMM" (o PMm). Quando clicco all'esterno, cambia in "2:15 AM". Riesco a salvare il report, ma quando riapro il report salvato, l'orario di programmazione appare come AM (ovvero mattina), indipendentemente dal fatto che abbia inserito AM o PM nell'orario di programmazione.	Reinserire l'orario programmato, facendo attenzione a non digitare tutti i caratteri "AM" o "PM"; è sufficiente digitare "A" per "AM" o "P" per "PM". Se non viene visualizzato il carattere aggiuntivo, l'orario di programmazione sarà impostato correttamente.

Risorse

Ulteriori suggerimenti per la risoluzione dei problemi possono essere trovati nel"Base di conoscenza NetApp" (è richiesto l'accesso al supporto).

Ulteriori informazioni di supporto sono disponibili in Data Infrastructure Insights"Supporto" pagina.

Se disponi di un abbonamento attivo a Data Infrastructure Insights, puoi utilizzare queste opzioni di supporto:

"Telefono" "Ticket di supporto"

Per maggiori informazioni, vedere il "Documentazione di supporto per Data Infrastructure Insights" .

Risoluzione dei problemi dell'unità di acquisizione su Linux

Qui troverete suggerimenti per la risoluzione dei problemi relativi alle unità di acquisizione su un server Linux.

Problema:	Prova questo:
Lo stato AU nella pagina **Osservabilità > Collezionisti** nella scheda **Unità di acquisizione** visualizza "Certificato scaduto" o "Certificato revocato".	Fare clic sul menu a destra dell'AU e selezionare **Ripristina connessione**. Seguire le istruzioni per ripristinare l'unità di acquisizione: 1. Interrompere il servizio Unità di acquisizione (AU). È possibile fare clic sul pulsante *Copia comando di arresto* per copiare rapidamente il comando negli appunti, quindi incollarlo in un prompt dei comandi sul computer dell'unità di acquisizione. 2. Creare un file denominato "token" nella cartella */var/lib/netapp/cloudinsights/acq/conf* sull'AU. 3. Fare clic sul pulsante *Copia token* e incollare il token nel file creato. 4. Riavviare il servizio AU. Fare clic sul pulsante *Copia comando di riavvio* e incollare il comando in un prompt dei comandi sull'AU.
Autorizzazione negata all'avvio del servizio Acquisition Unit Server	Quando l'AU è installato su SELINUX, SE deve essere impostato in modalità *permissiva*. La modalità *Enforcing* non è supportata. Dopo aver impostato SELINUX in modalità permissiva, riavviare il servizio AU.
Requisiti del server non soddisfatti	Assicurati che il tuo server o VM dell'unità di acquisizione soddisfi"requisiti"
Requisiti di rete non soddisfatti	Assicurati che il server/VM dell'unità di acquisizione possa accedere all'ambiente Data Infrastructure Insights (<nome-ambiente>.c01.cloudinsights.netapp.com) tramite connessione SSL sulla porta 443. Prova i seguenti comandi: *ping <nome-ambiente>.c01.cloudinsights.netapp.com traceroute <nome-ambiente>.c01.cloudinsights.netapp.com curl https://<nome-ambiente>.c01.cloudinsights.netapp.com wget https://<nome-ambiente>.c01.cloudinsights.netapp.com* Tieni presente che la porta 443 deve essere aperta "in uscita" dall'AU a Data Infrastructure Insights.
Server proxy non configurato correttamente	Verificare le impostazioni proxy e, se necessario, disinstallare/reinstallare il software Acquisition Unit per immettere le impostazioni proxy corrette. 1. Prova "arricciatura". Fare riferimento alle informazioni/documentazione di "man curl" relative ai proxy: --preproxy, --proxy-* (è un carattere jolly "*" perché curl supporta molte impostazioni proxy). 2. Prova "wget". Consultare la documentazione per le opzioni proxy.

L’installazione dell’unità di acquisizione non è riuscita in Data Infrastructure Insights con errori di credenziali durante l’avvio del servizio di acquisizione (e visibili in acq.log).	Ciò può essere causato dall’inclusione di caratteri speciali nelle credenziali del proxy. Disinstallare l’AU (*sudo cloudinsights-uninstall.sh*) e reinstallarlo senza utilizzare caratteri speciali.
Linux: libreria mancante / file non trovato	Assicurati che il tuo server/VM Linux Acquisition Unit disponga di tutte le librerie necessarie. Ad esempio, è necessario che sul server sia installata la libreria *unzip*. Per installare la libreria *unzip*, eseguire il comando **sudo yum install unzip** prima di eseguire lo script di installazione di Acquisition Unit
Problemi di autorizzazione	Assicurati di aver effettuato l’accesso come utente con autorizzazioni *sudo*
Acquisizione non in esecuzione:	Raccogli acq.log da /opt/netapp/cloudinsights/acq/logs (Linux) Riavvia il servizio di acquisizione: sudo cloudinsights-service.sh restart acquisition
Problemi di raccolta dati:	Invia un rapporto di errore dalla landing page di Data Collector cliccando sul pulsante "Invia rapporto di errore"
Stato: Heartbeat non riuscito	L’unità di acquisizione (AU) invia un heartbeat a Data Infrastructure Insights ogni 60 secondi per rinnovare il contratto di locazione. Se la chiamata heartbeat fallisce a causa di un problema di rete o Data Infrastructure Insights non reattivo, il tempo di lease dell’AU non viene aggiornato. Quando scade il periodo di leasing dell’AU, Data Infrastructure Insights mostra lo stato "Heartbeat Failed". Passaggi per la risoluzione dei problemi: verificare la connessione di rete tra il server dell’unità di acquisizione e CloudInsights. Verificare se il servizio Acquisition Unit è in esecuzione. Se il servizio non è in esecuzione, avviarlo. Controllare il registro dell’unità di acquisizione (/var/log/netapp/cloudinsights/acq/acq.log) per verificare se sono presenti errori.
Vedo un messaggio "Errore heartbeat:"	Questo errore può verificarsi se si verifica un’interruzione di rete che interrompe la comunicazione tra l’unità di acquisizione e l’ambiente Data Infrastructure Insights per più di un minuto. Verificare che la connessione tra AU e Data Infrastructure Insights sia stabile e attiva.
Quando reinstallo l’unità di acquisizione, visualizzo il messaggio "ValueError: contesto file per /opt/netapp/cloudinsights(/.*)? già definito".	Su un sistema con SELinux, questo messaggio di errore potrebbe apparire dopo `cloudinsights-uninstall.sh -p` è stato eseguito e l’Unità di acquisizione deve essere reinstallata. Esecuzione del comando `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` dovrebbe correggere il problema e rimuovere il messaggio.

Considerazioni su proxy e firewall

Se la tua organizzazione richiede l'utilizzo di un proxy per l'accesso a Internet, potrebbe essere necessario comprendere il comportamento del proxy della tua organizzazione e cercare determinate eccezioni affinché Data Infrastructure Insights funzioni. Tieni presente quanto segue:

- Innanzitutto, la tua organizzazione blocca l'accesso per impostazione predefinita e consente l'accesso solo a specifici siti web/domini in via eccezionale? In tal caso, sarà necessario aggiungere il seguente dominio all'elenco delle eccezioni:

  ```
  *.cloudinsights.netapp.com
  ```

  La tua Data Infrastructure Insights Acquisition Unit, così come le tue interazioni in un browser web con Data Infrastructure Insights, saranno tutte indirizzate agli host con quel nome di dominio.

- In secondo luogo, alcuni proxy tentano di eseguire l'ispezione TLS/SSL impersonando i siti Web Data Infrastructure Insights con certificati digitali non generati da NetApp. Il modello di sicurezza della Data Infrastructure Insights Acquisition Unit è fondamentalmente incompatibile con queste tecnologie. Sarà inoltre necessario escludere il nome di dominio sopra indicato da questa funzionalità affinché l'unità di acquisizione Data Infrastructure Insights possa accedere correttamente a Data Infrastructure Insights e facilitare l'individuazione dei dati.

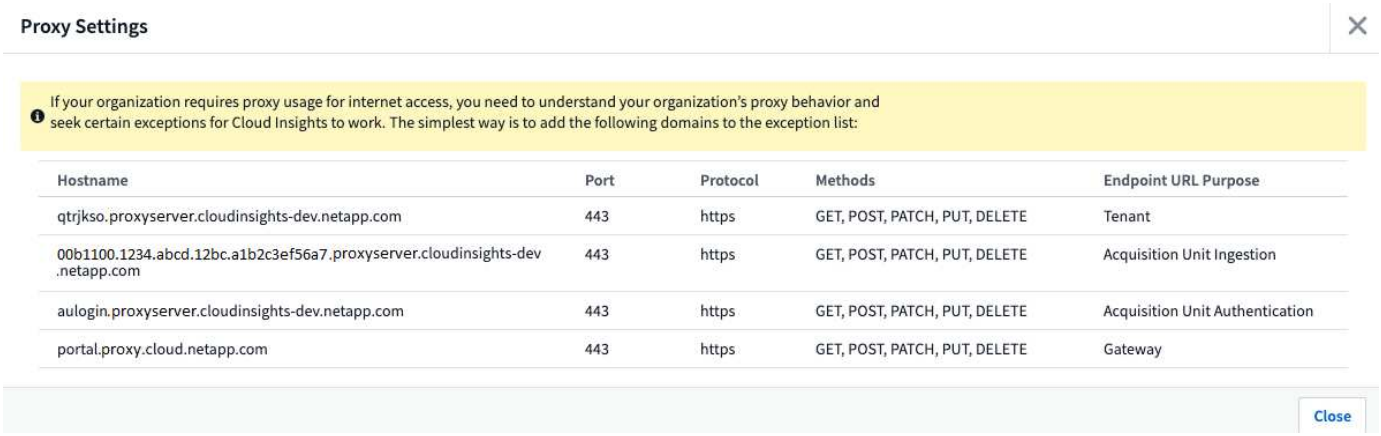
Nel caso in cui il proxy sia configurato per l'ispezione del traffico, l'ambiente Data Infrastructure Insights deve essere aggiunto a un elenco di eccezioni nella configurazione del proxy. Il formato e la configurazione di questo elenco di eccezioni variano a seconda dell'ambiente proxy e degli strumenti utilizzati, ma in generale è necessario aggiungere gli URL dei server Data Infrastructure Insights a questo elenco di eccezioni per consentire all'AU di comunicare correttamente con tali server.

Il modo più semplice per farlo è aggiungere il dominio Data Infrastructure Insights all'elenco delle eccezioni:

```
 *.cloudinsights.netapp.com
Nel caso in cui il proxy non sia impostato per l'ispezione del traffico,
potrebbe essere necessario o meno un elenco di eccezioni.  Se non sei
sicuro se devi aggiungere Data Infrastructure Insights a un elenco di
eccezioni o se riscontri difficoltà nell'installazione o nell'esecuzione
Data Infrastructure Insights a causa della configurazione del proxy e/o
del firewall, rivolgiti al team di amministrazione del proxy per
configurare la gestione dell'intercettazione SSL da parte del proxy.
```

Visualizzazione degli endpoint proxy

Puoi visualizzare gli endpoint proxy facendo clic sul collegamento **Impostazioni proxy** quando scegli un raccoglitore dati durante l'onboarding oppure sul collegamento in *Impostazioni proxy* nella pagina **Guida > Supporto**. Viene visualizzata una tabella come la seguente. Se nel tuo ambiente è presente Workload Security, in questo elenco verranno visualizzati anche gli URL degli endpoint configurati.



Risorse

Ulteriori suggerimenti per la risoluzione dei problemi possono essere trovati nel"Base di conoscenza NetApp" (è richiesto l'accesso al supporto).

Ulteriori informazioni di supporto sono disponibili in Data Infrastructure Insights"Supporto" pagina.

Risoluzione dei problemi dell'unità di acquisizione su Windows

Qui troverete suggerimenti per la risoluzione dei problemi relativi alle unità di acquisizione su un server Windows.

Problema:	Prova questo:
Lo stato AU nella pagina **Osservabilità > Collezionisti** nella scheda **Unità di acquisizione** visualizza "Certificato scaduto" o "Certificato revocato".	Fare clic sul menu a destra dell'AU e selezionare **Ripristina connessione**. Seguire le istruzioni per ripristinare l'unità di acquisizione: 1. Interrompere il servizio Unità di acquisizione (AU). È possibile fare clic sul pulsante *Copia comando di arresto* per copiare rapidamente il comando negli appunti, quindi incollarlo in un prompt dei comandi sul computer dell'unità di acquisizione. 2. Creare un file denominato "token" nella cartella *c:\Program Files\ Cloud Insights\Acquisition Unit\conf* sull'AU. 3. Fare clic sul pulsante *Copia token* e incollare il token nel file creato. 4. Riavviare il servizio AU. Fare clic sul pulsante *Copia comando di riavvio* e incollare il comando in un prompt dei comandi sull'AU.
Requisiti del server non soddisfatti	Assicurati che il tuo server o VM dell'unità di acquisizione soddisfi"requisiti"

Requisiti di rete non soddisfatti	Assicurati che il server/VM dell'unità di acquisizione possa accedere all'ambiente Data Infrastructure Insights (<nome-ambiente>.c01.cloudinsights.netapp.com) tramite connessione SSL sulla porta 443. Prova i seguenti comandi: *ping <nome-ambiente>.c01.cloudinsights.netapp.com traceroute <nome-ambiente>.c01.cloudinsights.netapp.com curl https://<nome-ambiente>.c01.cloudinsights.netapp.com wget https://<nome-ambiente>.c01.cloudinsights.netapp.com* Tieni presente che la porta 443 deve essere aperta "in uscita" dall'AU a Data Infrastructure Insights.
Server proxy non configurato correttamente	Verificare le impostazioni proxy e, se necessario, disinstallare/reinstallare il software Acquisition Unit per immettere le impostazioni proxy corrette. 1. Prova "arricciatura". Fare riferimento alle informazioni/documentazione di "man curl" relative ai proxy: --preproxy, --proxy-* (è un carattere jolly "*" perché curl supporta molte impostazioni proxy). 2. Prova "wget". Consultare la documentazione per le opzioni proxy.
L'installazione dell'unità di acquisizione non è riuscita in Data Infrastructure Insights con errori di credenziali durante l'avvio del servizio di acquisizione (e visibili in acq.log).	Ciò può essere causato dall'inclusione di caratteri speciali nelle credenziali del proxy. Disinstallare l'AU (*sudo cloudinsights-uninstall.sh*) e reinstallarlo senza utilizzare caratteri speciali.
Problemi di autorizzazione	Assicurati di aver effettuato l'accesso come utente con autorizzazioni di amministratore
Acquisizione non in esecuzione	È possibile trovare informazioni nel file acq.log nella cartella *<directory di installazione>\ Cloud Insights\Acquisition Unit\log*. Riavviare l'acquisizione tramite i servizi di Windows
Problemi di raccolta dati	Invia un rapporto di errore dalla landing page di Data Collector cliccando sul pulsante "Invia rapporto di errore"

Stato: Heartbeat non riuscito	L'unità di acquisizione (AU) invia un heartbeat a Data Infrastructure Insights ogni 60 secondi per rinnovare il contratto di locazione. Se la chiamata heartbeat fallisce a causa di un problema di rete o Data Infrastructure Insights non reattivo, il tempo di lease dell'AU non viene aggiornato. Quando scade il periodo di leasing dell'AU, Data Infrastructure Insights mostra lo stato "Heartbeat Failed". Passaggi per la risoluzione dei problemi: * Verificare la connessione di rete tra il server dell'unità di acquisizione e CloudInsights. * Verificare se il servizio Unità di acquisizione è in esecuzione. Se il servizio non è in esecuzione, avviarlo. * Controllare il registro dell'unità di acquisizione (<directory di installazione>:\Programmi\ Cloud Insights\Acquisition Unit\log\acq.log) per verificare se sono presenti errori.
Vedo un messaggio "Errore heartbeat:	Questo errore può verificarsi se si verifica un'interruzione di rete che interrompe la comunicazione tra l'unità di acquisizione e l'ambiente Data Infrastructure Insights per più di un minuto. Verificare che la connessione tra AU e Data Infrastructure Insights sia stabile e attiva.

Considerazioni su proxy e firewall

Se la tua organizzazione richiede l'utilizzo di un proxy per l'accesso a Internet, potrebbe essere necessario comprendere il comportamento del proxy della tua organizzazione e cercare determinate eccezioni affinché Data Infrastructure Insights funzioni. Tieni presente quanto segue:

- Innanzitutto, la tua organizzazione blocca l'accesso per impostazione predefinita e consente l'accesso solo a specifici siti web/domini in via eccezionale? In tal caso, dovrai aggiungere il seguente dominio all'elenco delle eccezioni:

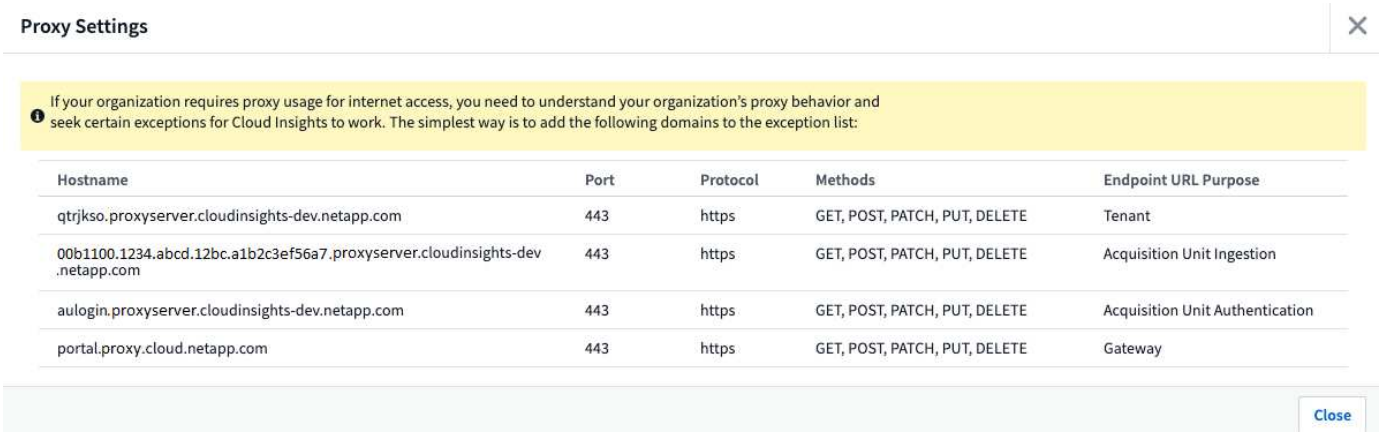
  ```
  *.cloudinsights.netapp.com
  ```

  La tua Data Infrastructure Insights Acquisition Unit, così come le tue interazioni in un browser web con Data Infrastructure Insights, saranno tutte indirizzate agli host con quel nome di dominio.

- In secondo luogo, alcuni proxy tentano di eseguire l'ispezione TLS/SSL impersonando i siti Web Data Infrastructure Insights con certificati digitali non generati da NetApp. Il modello di sicurezza della Data Infrastructure Insights Acquisition Unit è fondamentalmente incompatibile con queste tecnologie. Sarà inoltre necessario escludere il nome di dominio sopra indicato da questa funzionalità affinché l'unità di acquisizione Data Infrastructure Insights possa accedere correttamente a Data Infrastructure Insights e facilitare l'individuazione dei dati.

Visualizzazione degli endpoint proxy

Puoi visualizzare gli endpoint proxy facendo clic sul collegamento **Impostazioni proxy** quando scegli un raccoglitore dati durante l'onboarding oppure sul collegamento in *Impostazioni proxy* nella pagina **Guida > Supporto**. Viene visualizzata una tabella come la seguente. Se nel tuo ambiente è presente Workload Security, in questo elenco verranno visualizzati anche gli URL degli endpoint configurati.



Risorse

Ulteriori suggerimenti per la risoluzione dei problemi possono essere trovati nel"Base di conoscenza NetApp" (è richiesto l'accesso al supporto).

Ulteriori informazioni di supporto sono disponibili in Data Infrastructure Insights"Supporto" pagina.

Ricerca di un raccoglitore di dati fallito

Se un raccoglitore dati presenta un messaggio di errore e un impatto elevato o medio, è necessario analizzare il problema utilizzando la pagina di riepilogo del raccoglitore dati con le relative informazioni collegate.

Per determinare la causa del mancato funzionamento dei raccoglitori dati, attenersi alla seguente procedura. I messaggi di errore del Data Collector vengono visualizzati nel menu **Amministrazione** e nella pagina **Data Collector installati**.

Passi

1. Fare clic su **Amministrazione** > **Raccolta dati** > **Raccolta dati installati**.
2. Fare clic sul nome collegato del raccoglitore dati non riuscito per aprire la pagina Riepilogo.
3. Nella pagina Riepilogo, controlla l'area Commenti per leggere eventuali note lasciate da un altro tecnico che potrebbe stare indagando su questo guasto.
4. Annotare eventuali messaggi sulle prestazioni.
5. Sposta il puntatore del mouse sui segmenti del grafico della cronologia degli eventi per visualizzare informazioni aggiuntive.
6. Selezionare un messaggio di errore per un dispositivo visualizzato sotto la cronologia degli eventi e fare clic sull'icona Dettagli errore visualizzata a destra del messaggio.

   I dettagli dell'errore includono il testo del messaggio di errore, le cause più probabili, le informazioni in uso e i suggerimenti su cosa si può fare per correggere il problema.

7. Nell'area Dispositivi segnalati da questo raccoglitore dati, è possibile filtrare l'elenco per visualizzare solo i dispositivi di interesse e fare clic sul **Nome** collegato di un dispositivo per visualizzare la pagina delle risorse per quel dispositivo.
8. Quando torni alla pagina di riepilogo del raccoglitore dati, controlla l'area **Mostra modifiche recenti** in fondo alla pagina per verificare se le modifiche recenti potrebbero aver causato il problema.

Matrice di supporto del collettore dati Data Infrastructure Insights

La matrice di supporto del Data Collector fornisce un riferimento per i Data Collector supportati da Data Infrastructure Insights , comprese informazioni su fornitori e modelli.

Archiviazione HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
HPE Alletra 9080 HPE_3PAR 20450 HPE_3PAR 20800 HPE_3PAR 20850 HPE_3PAR 7200 HPE_3PAR 7200c HPE_3PAR 7400 HPE_3PAR 7400c HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR A650 HPE_3PAR A670 HP_3PAR 20800 HP_3PAR 7200 HP_3PAR 7200c HP_3PAR 7400 HP_3PAR 7400c HP_3PAR 7440c HP_3PAR 7450c HP_3PAR 8200 HP_3PAR 8400 HP_3PAR 8440 InServ F200 InServ F400 InServ T400 InServ T800 InServ V400 InServ V800	3.1.1 (MU1) 3.1.2 (MU3) 3.1.3 (MU1) 3.1.3 (MU2) 3.2.1 (MU2) 3.2.1 (MU3) 3.2.1 (MU5) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 3.3.1 (MU1) 3.3.1 (MU2) 3.3.1 (MU3) 3.3.1 (MU5) 3.3.2 (MU1) 4.3.1 4.3.3 4.4.1 Tipo di rilascio: rilascio di supporto standard 4.5.15 Tipo di rilascio: rilascio di supporto esteso 4.5.18 Tipo di rilascio: rilascio di supporto esteso 4.5.21 Tipo di rilascio: rilascio di supporto esteso 4.5.24 Tipo di rilascio: rilascio di supporto esteso 4.5.7 Tipo di rilascio: rilascio di supporto esteso 4.6.1 Tipo di rilascio: Rilascio con supporto esteso 9.5.15 Tipo di rilascio: Rilascio con supporto esteso 9.5.8 Tipo di rilascio: Rilascio con supporto esteso 9.6.1 Tipo di rilascio: Rilascio con supporto esteso

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
710					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità scritta	Implementato	SSH	Capacità totale scritta su questo volume
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Mappa del volume	LUN	Implementato	SSH	Nome del lun backend
		Controllore di protocollo	Implementato	SSH	
		Porto di archiviazione	Implementato	SSH	
		Tipo	Spacco	SSH	
	Maschera del volume	Iniziatore	Implementato	SSH	
		Controllore di protocollo	Implementato	SSH	
		Porto di archiviazione	Implementato	SSH	
		Tipo	Spacco	SSH	
	Riferimento volume	Nome	Implementato	SSH	
		IP di archiviazione	Implementato	SSH	
	Alias WWN	Alias host	Implementato	SSH	
		Tipo di oggetto	Implementato	SSH	
		Fonte	Implementato	SSH	
		WWN	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		blocco parziale			
		ID del server	Implementato	SMI-S	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Latenza di throughput	Implementato	SMI-S	
		Portata totale	Implementato	SMI-S	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	SMI-S	
		Scrivi in attesa	Implementato	SMI-S	scrittura totale in sospeso

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
3Par SMI-S	SMI-S	HTTP/HTTPS	5988/5989		VERO	VERO	VERO	VERO
3Par CLI	SSH	SSH	22		VERO	falso	VERO	VERO

Amazon AWS EC2

Modelli e versioni supportati da questo raccoglitore dati: Versioni API:

- 2014-10-01

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		OID del disco virtuale	Implementato	HTTPS	
		OID della macchina	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Ospite	Sistema operativo host	Implementato	HTTPS	
		IP	Implementato	HTTPS	
		Produttore	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		OID	Implementato	HTTPS	
	Informazioni	Descrizione dell'API	Implementato	HTTPS	
		Nome API	Implementato	HTTPS	
		Versione API	Implementato	HTTPS	
		Nome dell'origine dati	Implementato	HTTPS	Informazioni
		Data	Implementato	HTTPS	
		ID dell'originatore	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	macchina virtuale	Utilizzo totale della CPU	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		diskIops.totale	Implementato	HTTPS	
		Scrittura IOP su disco	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		Lettura della velocità effettiva del disco	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	velocità totale di lettura del disco
		Scrittura della velocità effettiva del disco	Implementato	HTTPS	
		Lettura della velocità effettiva IP	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Throughput IP totale
		ipThroughput.write	Implementato	HTTPS	
	Macchina virtuale	Capacità totale	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
EC2 API	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Amazon AWS S3

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
S3	2010-08-01

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Pool di archiviazione	Includi nella capacità DWH	Implementato	HTTPS	Un modo da ACQ per controllare quali pool di archiviazione sono interessanti in DWH Capacity
		Nome	Implementato	HTTPS	
		Capacità del disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità grezza per il pool di archiviazione
		Gruppo di incursione	Implementato	HTTPS	indica se questo storagePool è un gruppo raid
		Rapporto grezzo/utilizzabile	Implementato	HTTPS	rapporto per convertire dalla capacità utilizzabile alla capacità grezza
		ID pool di archiviazione	Implementato	HTTPS	
		Thin Provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione	Volume interno	Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Totale oggetti	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
S3 API	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Azure NetApp Files

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli
2019-06-01 2024-07-01	Azure NetApp Files

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		assegnata			
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
		Commento	Spacco	HTTPS	stato: commento di testo libero che descrive l'svm

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Disco StoragePool	IOP letti	Implementato		Numero di IOPS di lettura sul disco
		Scrittura IOP	Implementato		
		Lettura di throughput	Implementato		
		Scrittura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		IOP totali	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Azure NetApp Files	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Switch Fibre Channel Brocade

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
176,51 183,0 Brocade 200E Brocade 300E Brocade 4024 Embedded Brocade 5000 Brocade 5100 Brocade 5300 Brocade 5480 Embedded Brocade 6505 Brocade 6510 Brocade 6520 Brocade 6546 Brocade 6547 Embedded Brocade 6548 Brocade 6558 Brocade 7800 Brocade 7810 Extension Switch Brocade 7840 Brocade DCX Brocade DCX-4S Backbone Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade M5424 Embedded Brocade VA-40FC Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v6.2.2b v6.2.2f v6.2.2g v6.4.1b v6.4.2a v6.4.3 v6.4.3d v6.4.3f3 v7.0.1 v7.0.1b v7.0.2 v7.0.2b1 v7.0.2c v7.0.2e v7.0.2e1 v7.1.0a v7.1.0b v7.2.0a v7.2.0d v7.2.1 v7.2.1c v7.2.1c1 v7.2.1d v7.3.0a v7.3.0c v7.3.1 v7.3.1c v7.3.1d v7.3.2a v7.4.0a v7.4.1 v7.4.1d v7.4.1e v7.4.2 v7.4.2a v7.4.2a4 v7.4.2c v7.4.2d v7.4.2e v7.4.2f v7.4.2g v7.4.2g_cvr_824494_01 v7.4.2h v7.4.2j1 v8.0.2c v8.0.2d v8.0.2f v8.1.0b v8.1.1a v8.1.2a v8.1.2d v8.1.2f v8.1.2g v8.1.2h v8.1.2j v8.1.2k v8.2.0 v8.2.0a v8.2.0a1 v8.2.0b v8.2.1 v8.2.1a v8.2.1c v8.2.1d v8.2.2a v8.2.2b v8.2.2c v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3a1 v8.2.3a_cvr_855776_01 v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v8.2.3e2 v9.0.0a v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1 v9.1.1a v9.1.1b v9.1.1b_lw v9.1.1c v9.1.1d v9.1.1d1 v9.1.1d2 v9.1.1d2_lw v9.1.1d5 v9.2.0a v9.2.0b v9.2.0b1_lw v9.2.0c v9.2.0c1 v9.2.1a v9.2.1a1 v9.2.2

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
	Zona	Nome della zona	Implementato	SSH	
	Membro della zona	Tipo	Spacco	SSH	
		WWN	Implementato	SSH	
	Capacità di zonizzazione	Configurazione attiva	Implementato	SSH	
		Nome della configurazione	Implementato	SSH	
		Comportamento di zonizzazione predefinito	Implementato	SSH	
		WWN	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		segnale di errore della porta			segnale di errore della porta
		Errore di porta, parametri di configurazione	Implementato	SNMP	Errore di porta, informazioni aggiuntive
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Errore porta trasmissione scarto timeout	Implementato	SNMP	Errori di porta timeout scarta
		Errori totali della porta	Implementato	SNMP	Errori totali della porta
		ID del server	Implementato	SNMP	
		Frequenza dei fotogrammi del traffico	Implementato	SNMP	
		Frame rate totale del traffico	Implementato	SNMP	
		Frequenza dei fotogrammi del traffico	Implementato	SNMP	
		Dimensione media del telaio	Implementato	SNMP	Dimensione media del frame del traffico
		Cornici TX	Implementato	SNMP	dimensione media del frame del traffico
		Tasso di traffico ricevuto	Implementato	SNMP	
		Tasso di traffico totale	Implementato	SNMP	
		Velocità di trasmissione del traffico	Implementato	SNMP	
		Utilizzo del traffico ricevuto	Implementato	SNMP	
		Utilizzo totale del traffico	Implementato	SNMP	Utilizzo totale del traffico
		Utilizzo della trasmissione del traffico	Implementato	SNMP	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Brocade SNMP	SNMP	SNMPv1, SNMPv2, SNMPv3	161		VERO	VERO	VERO	VERO
Brocade SSH	SSH	SSH	22		falso	falso	VERO	VERO
Configurazione guidata origine dati	Inserimento manuale				VERO	VERO	VERO	VERO

Consulente di rete Brocade HTTP

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
14.4.3 14.4.4	Brocade 6520 Brocade DCX 8510-4 Brocade G620 Brocade X6-8 EMC Connectrix DS-6510B	v7.3.0b v7.4.1b v8.2.3c1 v9.0.1e1

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Connettività sconosciuta	Implementato	HTTP/S	
		Lama	Implementato	HTTP/S	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo GBIC	Implementato	HTTP/S	
	Interruttore	WWN	Implementato	HTTP/S	
		Proprietà intellettuale	Implementato	HTTP/S	
		Versione del firmware	Implementato	HTTP/S	
		Produttore	Implementato	HTTP/S	
		Modello	Implementato	HTTP/S	
		Nome	Implementato	HTTP/S	
		Cambia ruolo	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	
		Numero di serie	Implementato	HTTP/S	
		Gestisci URL	Implementato	HTTP/S	
		Cambia stato	Implementato	HTTP/S	
		Stato dell'interruttore	Implementato	HTTP/S	
		ID dominio	Implementato	HTTP/S	
		VSAN abilitato	Implementato	HTTP/S	
	Sconosciuto	WWN	Implementato	HTTP/S	
		Produttore	Implementato	HTTP/S	
		Firmware	Implementato	HTTP/S	
		Autista	Implementato	HTTP/S	
		Modello	Implementato	HTTP/S	
	Alias WWN	Alias host	Implementato	HTTP/S	
		Tipo di oggetto	Implementato	HTTP/S	
		Fonte	Implementato	HTTP/S	
		WWN	Implementato	HTTP/S	
	Zona	Nome della zona	Implementato	HTTP/S	
	Membro della zona	Tipo	Spacco	HTTP/S	
		WWN	Implementato	HTTP/S	
	Capacità di zonizzazione	Configurazione attiva	Implementato	HTTP/S	
		Nome della configurazione	Implementato	HTTP/S	
		WWN	Implementato	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione	porta	BB Credito Zero Trasmesso	Implementato	HTTP/S	BB Credito Zero Trasmesso
		BB Credito Zero Totale	Implementato	HTTP/S	BB Credito Zero Totale
		BB Credito Zero Ms Trasmesso	Implementato	HTTP/S	BB Credito Zero Ms Trasmesso

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Brocade Network Advisor	HTTP/HTTPS	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

Brocade FOS REST

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
183.0 184.0 190.0 Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7810 Switch di estensione Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v8.2.2a v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v9.0.0b v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1a v9.1.1b v9.1.1c v9.1.1c3 v9.1.1d v9.1.1d1 v9.1.1d1_lw v9.1.1d2 v9.1.1d3_cvr_861742_01 v9.2.0a v9.2.0b v9.2.0b1 v9.2.0b_cvr_857687_01 v9.2.0c v9.2.0c3 v9.2.1 v9.2.1a v9.2.1b v9.2.2

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
	Zona	Nome della zona	Implementato	HTTPS	
	Membro della zona	Tipo	Spacco	HTTPS	
		WWN	Implementato	HTTPS	
	Capacità di zonizzazione	Configurazione attiva	Implementato	HTTPS	
		Nome della configurazione	Implementato	HTTPS	
		Comportamento di zonizzazione predefinito	Implementato	HTTPS	
		WWN	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Errore di porta, perdita di sincronizzazione	Implementato	HTTPS	Errore di porta, perdita di sincronizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		ID del server	Implementato	HTTPS	
		Frequenza dei fotogrammi del traffico	Implementato	HTTPS	
		Frame rate totale del traffico	Implementato	HTTPS	
		Frequenza dei fotogrammi del traffico	Implementato	HTTPS	
		Dimensione media del telaio	Implementato	HTTPS	Dimensione media del frame del traffico
		Cornici TX	Implementato	HTTPS	dimensione media del frame del traffico
		Tasso di traffico ricevuto	Implementato	HTTPS	
		Tasso di traffico totale	Implementato	HTTPS	
		Velocità di trasmissione del traffico	Implementato	HTTPS	
		Utilizzo del traffico ricevuto	Implementato	HTTPS	
		Utilizzo totale del traffico	Implementato	HTTPS	Utilizzo totale del traffico
		Utilizzo della trasmissione del traffico	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST FOS Brocade	HTTPS		443		VERO	VERO	VERO	VERO

Switch Cisco MDS e Nexus Fabric

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
DS-C9124-2-K9 DS-C9124-K9 DS-C9132T-K9 DS-C9148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148T-K9 DS-C9148V-K9 DS-C9220I-K9 DS-C9222I-K9 DS-C9250I-K9 DS-C9396S-K9 DS-C9396T-K9 DS-C9396V-K9 DS-C9506 DS-C9509 DS-C9513 DS-C9706 DS-C9710 DS-C9718 DS-HP-8GFC-K9 DS-HP-FC-K9 N5K-C5548UP N5K-C5596UP N5K-C5696Q UCS-FI-6248UP UCS-FI-6296UP UCS-FI-6332 UCS-FI-6332-16UP UCS-FI-64108 UCS-FI-6454	3.3(1c) 4.1(3a) 4.2(1a) 5.0(1a) 5.0(3)N2(3.11e) 5.0(3)N2(4.01d) 5.0(3)N2(4.13i) 5.0(3)N2(4.21e) 5.0(3)N2(4.21j) 5.0(3)N2(4.21k) 5.0(3)N2(4.22c) 5.0(3)N2(4.23f) 5.0(3)N2(4.23g) 5.0(3)N2(4.34a) 5.0(8) 5.2(2d) 5.2(8) 5.2(8a) 5.2(8b) 5.2(8c) 5.2(8d) 5.2(8f) 5.2(8g) 5.2(8h) 5.2(8i) 6.2(11) 6.2(11b) 6.2(11c) 6.2(13) 6.2(13a) 6.2(15) 6.2(17) 6.2(19) 6.2(21) 6.2(23) 6.2(25) 6.2(27) 6.2(29) 6.2(31) 6.2(33) 6.2(5a) 6.2(7) 6.2(9) 6.2(9a) 6.2(9b) 7.0(3)N2(4.04e) 7.0(3)N2(4.13b) 7.0(3)N2(4.13g) 7.3(0)D1(1) 7.3(1)DY(1) 7.3(13)N1(1) 7.3(8)N1(1) 8.1(1) 8.1(1a) 8.2(1) 8.2(2) 8.3(1) 8.3(2) 8.4(1) 8.4(1a) 8.4(2) 8.4(2a) 8.4(2b) 8.4(2c) 8.4(2d) 8.4(2e) 8.4(2f) 8.5(1) 9.2(1a) 9.2(2) 9.3(1) 9.3(2) 9.3(2a) 9.3(5)I42(1b) 9.3(5)I42(1g) 9.3(5)I42(1j) 9.3(5)I42(1k) 9.3(5)I42(3f) 9.3(5)I43(4b) 9.4(1) 9.4(1a) 9.4(2) 9.4(2a) 9.4(3)

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Tipo	Spacco	SNMP	
		VSAN abilitato	Implementato	SNMP	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		WWN	Implementato	SNMP	
	Sconosciuto	Autista	Implementato	SNMP	
		Firmware	Implementato	SNMP	
		Generato	Implementato	SNMP	
		Produttore	Implementato	SNMP	
		Modello	Implementato	SNMP	
		Nome	Implementato	SNMP	
		WWN	Implementato	SNMP	
	Alias WWN	Alias host	Implementato	SNMP	
		Tipo di oggetto	Implementato	SNMP	
		Fonte	Implementato	SNMP	
		WWN	Implementato	SNMP	
	Zona	Nome della zona	Implementato	SNMP	
		Tipo di zona	Implementato	SNMP	
	Membro della zona	Tipo	Spacco	SNMP	
		WWN	Implementato	SNMP	
	Capacità di zonizzazione	Configurazione attiva	Implementato	SNMP	
		Nome della configurazione	Implementato	SNMP	
		Comportamento di zonizzazione predefinito	Implementato	SNMP	
		Controllo unione	Implementato	SNMP	
		WWN	Implementato	SNMP	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		scarto timeout			
		Errori totali della porta	Implementato	SNMP	Errori totali della porta
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tabella server	Implementato	SNMP	
		Frequenza dei fotogrammi del traffico	Implementato	SNMP	
		Frame rate totale del traffico	Implementato	SNMP	
		Frequenza dei fotogrammi del traffico	Implementato	SNMP	
		Dimensione media del telaio	Implementato	SNMP	Dimensione media del frame del traffico
		Cornici TX	Implementato	SNMP	dimensione media del frame del traffico
		Tasso di traffico ricevuto	Implementato	SNMP	
		Tasso di traffico totale	Implementato	SNMP	
		Velocità di trasmissione del traffico	Implementato	SNMP	
		Utilizzo del traffico ricevuto	Implementato	SNMP	
		Utilizzo totale del traffico	Implementato	SNMP	Utilizzo totale del traffico
		Utilizzo della trasmissione del traffico	Implementato	SNMP	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Cisco SNMP	SNMP	SNMPv1 (solo inventario), SNMPv2, SNMPv3	161		VERO	VERO	VERO	VERO

Coesità

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
Nodo di calcolo C4000 C4600 C5036 C5066 C6025 C6035 C6055 CX8405 PXG1 UCS-C240M5H10 Virtual ROBO	6.8.1_u1_release-20221022_6f58ed2a 6.8.2_u1_release-20240509_a5da4644 7.1.2_u2_release-20240925_66722648 7.1.2_u3_release-20241231_bb47fe77 7.2.1_release-20241114_794eae46 7.2.2_release-20250228_63e93ccf

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
780					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					livello del volume sopra di esso
Prodotto	**Categoria**	**Capacità totale/attribuita**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità totale utilizzata	Implementato		Capacità totale in MB
		Tipo	Spacco		
		Virtuale	Implementato		Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
		Criptato	Implementato		
prestazione	Magazzinaggio	Capacità grezza non riuscita	Implementato		
		Capacità grezza	Implementato		
		Capacità grezza di riserva	Implementato		Capacità grezza dei dischi di riserva (somma di tutti i dischi di riserva)
		Capacità di StoragePools	Implementato		
		IOP letti	Implementato		Numero di IOPS di lettura sul disco
		IOP totali	Implementato		
		Scrittura IOP	Implementato		
		Chiave	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Latenza di scrittura	Implementato		
		ID del server	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		
		Utilizzo totale	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Cohesity	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

EMC Celerra (SSH)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
NSX VG8 VNX5200 VNX5300 VNX5400 VNX5500	5.5.38-1 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.9-155

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					supporta il provisioning sottile per il volume
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità totale assegnata	Implementato	SSH	
		Capacità totale utilizzata	Implementato	SSH	Capacità totale in MB
		Tipo	Spacco	SSH	
		Virtuale	Implementato	SSH	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

API di gestione utilizzate da questo raccoglitore dati:

API	**Protocollo utilizzato**	**Protocollo di livello di trasporto utilizzato**	**Porte in entrata utilizzate**	**Porte in uscita utilizzate**	**Supporta l'autenticazione**	**Richiede solo credenziali di "sola lettura"**	**Supporta la crittografia**	**Compatibile con firewall (porte statiche)**
Celerra CLI	SSH	SSH			VERO	falso	VERO	VERO

EMC CLARiiON (NaviCLI)

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	**Modelli**	**Versioni del firmware**
6.26 6.28 7.32 7.33	CX3-40f CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600	04.28.000.5.710 05.32.000.5.206 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.32.000.5.249 05.33.000.5.074 05.33.008.5.119 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266 05.33.021.5.322 3.26.40.5.029

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		ID pool di archiviazione	Implementato	Interfaccia a riga di comando	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Alias WWN	Alias host	Implementato	Interfaccia a riga di comando	
		Proprietà intellettuale	Implementato	Interfaccia a riga di comando	
		Tipo di oggetto	Implementato	Interfaccia a riga di comando	
		Fonte	Implementato	Interfaccia a riga di comando	
		WWN	Implementato	Interfaccia a riga di comando	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Utilizzo totale	Implementato	Interfaccia a riga di comando	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Rapporto di lettura della cache	Implementato	Interfaccia a riga di comando	
		Rapporto di hit della cache totale	Implementato	Interfaccia a riga di comando	
		Rapporto di hit della cache in scrittura	Implementato	Interfaccia a riga di comando	
		Capacità grezza	Implementato	Interfaccia a riga di comando	
		Capacità totale	Implementato	Interfaccia a riga di comando	
		Capacità utilizzata	Implementato	Interfaccia a riga di comando	
		Rapporto di capacità utilizzata	Implementato	Interfaccia a riga di comando	
		IOP letti	Implementato	Interfaccia a riga di comando	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	Interfaccia a riga di comando	
		Scrittura IOP	Implementato	Interfaccia a riga di comando	
		Latenza di lettura	Implementato	Interfaccia a riga di comando	
		Latenza totale	Implementato	Interfaccia a riga di comando	
		Latenza di scrittura	Implementato	Interfaccia a riga di comando	
		Rapporto di blocco parziale	Implementato	Interfaccia a riga di comando	
		Lettura di throughput	Implementato	Interfaccia a riga di comando	
		Portata totale	Implementato	Interfaccia a riga di comando	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	Interfaccia a riga di comando	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Interfaccia a riga di comando di Navi	Interfaccia a riga di comando		6389,2162,2163,443(HTTPS)/80(HTTP)		VERO	VERO	VERO	falso

Dominio dati EMC (SSH)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
DD VE DD2500 DD3300 DD4200 DD6300 DD6400 DD6800 DD6900 DD7200 DD9300 DD9400 DD9410 DD9500 DD9800 DD990 DD9900 DD9910	6.0.2.30-606339 6.1.2.051-633576 6.1.2.20-606786 6.2.1.30-663869 6.2.1.40-671977 6.2.1.60-686365 7.10.0.20-1023227 7.10.1.0-1042928 7.10.1.1-1049892 7.10.1.10-1068159 7.10.1.15-1078832 7.10.1.20-1090468 7.10.1.30-1105324 7.10.1.40-1126469 7.10.1.50-1146826 7.11.0.0-1035502 7.13.0.20-1082704 7.2.0.20-658029 7.2.0.60-682124 7.2.0.70-686759 7.2.0.90-692270 7.7.4.0-1017976 7.7.5.1-1040473 7.7.5.11-1046187 7.7.5.25-1078970 7.7.5.30-1091295 8.0.0.10-1097914 8.1.0.10-1127744

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					capacità utilizzabile alla capacità grezza
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Thin Provisioning supportato	Implementato	SSH	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	SSH	
		Capacità totale utilizzata	Implementato	SSH	Capacità totale in MB
		Tipo	Spacco	SSH	
		Virtuale	Implementato	SSH	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
CLI di Data Domain	SSH	SSH	22		VERO	VERO	VERO	VERO

EMC ECS

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
ECS	3.6.1.3 3.6.2.1 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.6 3.8.0.1 3.8.0.2 3.8.0.3 3.8.0.4 3.8.0.5 3.8.0.6 3.8.1.1 3.8.1.2 3.8.1.3

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		nodo utilizzabile in MB			
		Utilizzo della capacità in MB	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Pool di archiviazione	Includi nella capacità DWH	Implementato	HTTPS	Un modo da ACQ per controllare quali pool di archiviazione sono interessanti in DWH Capacity
		Nome	Implementato	HTTPS	
		Capacità del disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità grezza per il pool di archiviazione
		Gruppo di incursione	Implementato	HTTPS	indica se questo storagePool è un gruppo raid
		Rapporto grezzo/utilizzabile	Implementato	HTTPS	rapporto per convertire dalla capacità utilizzabile alla capacità grezza
		ID pool di archiviazione	Implementato	HTTPS	
		Thin Provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Disco StoragePool	Capacità fornita	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità di impegno eccessivo	Implementato	HTTPS	Segnalato come serie temporale
		Rapporto di capacità utilizzata	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC ECS	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Dell EMC Isilon e PowerScale Rest

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
A100 A200 A2000 A300 A3000 F200 F600 F800 F900 H400 H500 H5600 H600 H700 NL410 S210 X210 X410	9.1.0.10 9.1.0.6 9.1.0.9 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.13 9.2.1.19 9.2.1.4 9.2.1.9 9.4.0.11 9.4.0.13 9.4.0.14 9.4.0.15 9.4.0.16 9.4.0.17 9.4.0.18 9.5.0.3 9.5.0.5 9.5.0.6 9.5.0.7 9.5.0.8 9.5.1.0 9.5.1.1 9.5.1.2 9.7.1.0 9.7.1.2 9.7.1.3 9.7.1.4 9.7.1.5 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.1.0.4 v8.1.2.0 v9.0.0.0

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					capacità grezza
		Capacità allocata	Spacco	HTTPS	Capacità allocata in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità utilizzata istantanea	Implementato	HTTPS	
		ID pool di archiviazione	Implementato	HTTPS	
		Thin Provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
840					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		capacità utilizzata istantanea			
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Latenza di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC Isilon e PowerScale	HTTPS		443		VERO	VERO	VERO	VERO

Dell EMC Isilon / PowerScale (CLI)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
A200 H400 H500 NL400 NL410 S210 Traceback (ultima chiamata): X200 X400 X410	9.1.0.18 9.1.0.19 9.2.1.12 9.2.1.13 9.2.1.15 9.4.0.17 9.5.0.3 9.5.0.6 9.5.0.8 9.7.1.2 9.8.0.2 v7.2.0.5 v7.2.1.3 v7.2.1.6 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.0.1.1 v8.1.2.0

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità totale assegnata	Implementato	SSH	
Prodotto	**Categoria**	**Capacità totale/attribuita**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	SSH	
		Virtuale	Implementato	SSH	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					dischi) in MB/s
		Scrittura di throughput	Implementato	SSH	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Utilizzo totale	Implementato	SSH	
	Disco StoragePool	Capacità totale	Implementato	SSH	
		Rapporto di capacità utilizzata	Implementato	SSH	
		Capacità totale dei dati	Implementato	SSH	
		Capacità fornita	Implementato	SSH	
		Capacità dati utilizzata	Implementato	SSH	
		Capacità utilizzata	Implementato	SSH	
		Capacità grezza	Implementato	SSH	
		Rapporto di capacità di impegno eccessivo	Implementato	SSH	Segnalato come serie temporale
		Capacità utilizzata istantanea	Implementato	SSH	
		Capacità riservata snapshot	Implementato	SSH	
		Rapporto di capacità utilizzata istantanea	Implementato	SSH	Segnalato come serie temporale

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Isilon SSH	SSH	SSH	22		VERO	falso	VERO	VERO

EMC PowerStore REST

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5200T PowerStore 9000T PowerStore 9200T	2.1.0.1 2.1.1.0 3.2.0.1 3.2.1.0 3.2.1.1 3.5.0.1 3.5.0.2 3.6.0.0 3.6.1.0 3.6.1.1 3.6.1.2 3.6.1.3 3.6.1.4 4.0.0.1 4.0.0.2 4.0.1.0

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato		Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato		Snapshot Capacità utilizzata in MB
		Percorso di giunzione	Implementato		
		Nome	Implementato		
		Capacità grezza totale	Implementato		Capacità grezza totale (somma di tutti i dischi nell'array)
		ID pool di archiviazione	Implementato		
		Fornito in modo sottile	Implementato		
		Tipo	Spacco		
		UUID	Implementato		
		Capacità utilizzata	Implementato		
		QoS - Politica	Implementato		
	Mappa del volume	LUN	Implementato		Nome del lun backend
		Mascheratura obbligatoria	Implementato		
		Controllore di protocollo	Implementato		
		Porto di archiviazione	Implementato		
		Tipo	Spacco		
	Maschera del volume	Iniziatore	Implementato		
		Controllore di protocollo	Implementato		
		Tipo	Spacco		
	Alias WWN	Alias host	Implementato		
		Tipo di oggetto	Implementato		
		Fonte	Implementato		
		WWN	Implementato		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità grezza	Implementato		
		Capacità totale	Implementato		
		Capacità utilizzata	Implementato		
		Rapporto di capacità utilizzata	Implementato		
		IOP letti	Implementato		Numero di IOPS di lettura sul disco
		IOP totali	Implementato		
		Scrittura IOP	Implementato		
		Chiave	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Latenza di scrittura	Implementato		
		ID del server	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di EMC PowerStore	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

EMC RecoverPoint (HTTP)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
RecoverPoint	5.1.SP4.P1(h.89) 5.1.SP4.P2(h.101) 5.1.SP4.P3(h.109) 5.1.SP4.P4(h.97) 5.1.SP4.P5(h.138)

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Nodo di archiviazione	Dimensione della memoria	Spacco	HTTPS	memoria del dispositivo in MB
		Modello	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Conteggio dei processori	Implementato	HTTPS	CPU del dispositivo
		Numero di serie	Implementato	HTTPS	
		Stato	Implementato	HTTPS	testo libero che descrive lo stato del dispositivo
		UUID	Implementato	HTTPS	
		Versione	Implementato	HTTPS	versione del software
	Sincronizzazione dell'archiviazione	Modalità	Implementato	HTTPS	
		Enumerazione modalità	Implementato	HTTPS	
		Archiviazione di origine	Implementato	HTTPS	
		Volume sorgente	Implementato	HTTPS	
		Stato	Implementato	HTTPS	testo libero che descrive lo stato del dispositivo
		Enum di Stato	Implementato	HTTPS	
		Archiviazione di destinazione	Implementato	HTTPS	
		Volume obiettivo	Implementato	HTTPS	
		Tecnologia	Implementato	HTTPS	tecnologia che causa l'efficienza di archiviazione cambiata

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di RecoverPoint	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

EMC ScaleIO e PowerFlex REST

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
ScaleIO	R3_5.1201.101 R3_6.1000.134

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato	HTTPS	Snapshot Capacità utilizzata in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità grezza totale	Implementato	HTTPS	Capacità grezza totale (somma di tutti i dischi nell'array)
		ID pool di archiviazione	Implementato	HTTPS	
		Fornito in modo sottile	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
		IP host	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione	Magazzinaggio	Capacità grezza non riuscita	Implementato		
		Capacità grezza	Implementato		
		Capacità grezza di riserva	Implementato		Capacità grezza dei dischi di riserva (somma di tutti i dischi di riserva)
		Capacità di StoragePools	Implementato		
		IOP letti	Implementato		Numero di IOPS di lettura sul disco
		IOP totali	Implementato		
		Scrittura IOP	Implementato		
		Chiave	Implementato		
		ID del server	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC ScaleIO e PowerFlex	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Interfaccia a riga di comando EMC Symmetrix

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
V10.0.0.0 V10.0.1.1 V10.1.0.0 V10.1.0.1 V10.1.0.3 V10.1.0.5 V10.2.0.0 V8.3.0.6 V8.4.0.7 V8.4.0.9 V9.1.0.5 V9.1.0.6 V9.2.1.0 V9.2.2.0 V9.2.3.0 V9.2.3.1 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.8	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5876.286.194(16F40000) build 115 5876.309.196(16F40000) build 153 5876.309.196(16F40000) build 162 5876.309.196(16F40000) build 94 5977.1151.1151(17590000) build 45 5977.1151.1151(17590000) build 60 5977.1151.1151(17590000) build 9 5978.711.711(175A0000) build 320 5978.711.711(175A0000) build 335 5978.711.711(175A0000) build 365 5978.711.711(175A0000) build 416 5978.711.711(175A0000) build 436 5978.711.711(175A0000) build 438 5978.711.711(175A0000) build 448 5978.711.711(175A0000) build 484 5978.711.711(175A0000) build 542 5978.711.711(175A0000) build 581 5978.714.714(175A0000) build 1 5978.714.714(175A0000) build 101 5978.714.714(175A0000) build 108 5978.714.714(175A0000) build 117 5978.714.714(175A0000) build 137 5978.714.714(175A0000) build 145 5978.714.714(175A0000) build 34 5978.714.714(175A0000) build 49 5978.714.714(175A0000) versione 53 5978.714.714(175A0000) versione 79

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
888					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		protocollo			
		Porto di archiviazione	Implementato		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco		
	Membro del volume	Livelli automatici	Implementato		indica se questo pool di archiviazione partecipa al tiering automatico con altri pool
		Capacità	Implementato		Snapshot Capacità utilizzata in MB
		Cilindri	Implementato		
		Nome	Implementato		
		Rango	Implementato		
		Capacità grezza totale	Implementato		Capacità grezza totale (somma di tutti i dischi nell'array)
		Ridondanza	Implementato		Livello di ridondanza
		ID pool di archiviazione	Implementato		
		UUID	Implementato		
	Riferimento volume	Nome	Implementato		
		IP di archiviazione	Implementato		
	Alias WWN	Alias host	Implementato		
		Tipo di oggetto	Implementato		
		Fonte	Implementato		
		WWN	Implementato		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Throughput	Implementato		
		Scrivi in attesa	Implementato		scrittura totale in sospeso

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
simcli	Interfaccia a riga di comando		2707		VERO	VERO	VERO	VERO
Symmetrix SMI-S	SMI-S	HTTP/HTTPS	5988/5989		VERO	falso	falso	VERO

Dell Unisphere REST

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
V10.0.0.5 V10.0.1.5 V10.1.0.1 V10.1.0.5 V10.1.0.6 V10.1.0.8 V10.2.0.1 V10.2.0.2 V9.2.3.15 V9.2.3.20 V9.2.3.22 V9.2.3.4 V9.2.4.1 V9.2.4.10 V9.2.4.11 V9.2.4.12 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.9	PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX200K VMAX250F VMAX400K VMAX450F VMAX950F	5977.1131.1131 build 615 5977.1151.1151 build 60 build 60 5978.711.711 build 205 5978.711.711 build 335 build 335 5978.711.711 build 365 5978.711.711 build 416 5978.711.711 build 436 build 436 5978.711.711 build 438 5978.711.711 build 448 5978.711.711 build 471 5978.711.711 build 484 5978.711.711 build 484 build 484 5978.711.711 build 542 5978.711.711 build 542 build 542 5978.711.711 build 581 5978.711.711 build 75 5978.711.711 build 8 build 8 5978.714.711 build 49 5978.714.714 build 1 build 1 5978.714.714 build 101 build 101 5978.714.714 build 108 5978.714.714 build 117 5978.714.714 build 117 build 117 5978.714.714 build 131 build 131 5978.714.714 build 137 5978.714.714 build 137 build 137 5978.714.714 build 145 5978.714.714 build 149 build 149 5978.714.714 build 34 5978.714.714 build 49 5978.714.714 build 49 build 49 5978.714.714 build 79 5978.714.714 build 79 build 79 6079.175.0 build 161 build 161 6079.175.0 build 259 build 259 6079.225.0 build 127 build 127 6079.225.0 build 216 build 216 6079.225.0 build 218 build 218 6079.225.0 build 291 build 291 6079.225.0 build 331 build 331 6079.225.0 build 86 build 86 6079.275.0 build 221 build 221

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità scritta	Implementato	HTTPS	Capacità totale scritta su questo volume
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Percentuale di capacità effettiva utilizzata	Implementato	HTTPS	
		Compressione abilitata	Implementato	HTTPS	
		gruppi di archiviazione	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Alias WWN	Alias host	Implementato	HTTPS	
		Tipo di oggetto	Implementato	HTTPS	
		Fonte	Implementato	HTTPS	
		WWN	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Chiave	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Scrittura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Latenza di lettura	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		Scrittura IOP	Implementato	HTTPS	
		IOP totali	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Risparmio totale sulla compressione	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API Dell Unisphere	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

EMC VNX (SSH)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
VNX5300 VNX5500 VNX5700	05.32.000.5.216 05.32.000.5.221 05.32.000.5.249 7.1.76-4 7.1.80-3

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
		archiviazione			
		Controllore di protocollo	Implementato	SSH	
		Tipo	Spacco	SSH	
	Maschera del volume	Porto di archiviazione	Implementato	SSH	
		Iniziatore	Implementato	SSH	
		Controllore di protocollo	Implementato	SSH	
		Tipo	Spacco	SSH	
	Membro del volume	Nome	Implementato	SSH	
		ID pool di archiviazione	Implementato	SSH	
		Rango	Implementato	SSH	
		Capacità	Implementato	SSH	Snapshot Capacità utilizzata in MB
		Capacità grezza totale	Implementato	SSH	Capacità grezza totale (somma di tutti i dischi nell'array)
		Capacità utilizzata	Implementato	SSH	
		Ridondanza	Implementato	SSH	Livello di ridondanza
	Alias WWN	Fonte	Implementato	SSH	
		Alias host	Implementato	SSH	
		WWN	Implementato	SSH	
		Tipo di oggetto	Implementato	SSH	
		Proprietà intellettuale	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità fornita	Implementato	SSH	
		Rapporto di capacità di	Implementato	SSH	Segnalato come serie temporale
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Latenza totale	Implementato	SSH	
		Rapporto di blocco parziale	Implementato	SSH	
		Latenza di lettura	Implementato	SSH	
		Scrittura IOP	Implementato	SSH	
		Lettura di throughput	Implementato	SSH	
		IOP totali	Implementato	SSH	
		Latenza di scrittura	Implementato	SSH	
		IOP letti	Implementato	SSH	Numero di IOPS di lettura sul disco
		Rapporto di lettura della cache	Implementato	SSH	
		Rapporto di hit della cache totale	Implementato	SSH	
		Rapporto di hit della cache in scrittura	Implementato	SSH	
		Scrittura di throughput	Implementato	SSH	
		Portata totale	Implementato	SSH	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
VNX SSH e CLI	SSH	SSH	22		VERO	falso	VERO	VERO

EMC VNXe e Unity Unisphere (CLI)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
Unità 300 Unità 300F Unità 350F Unità 380 Unità 380F Unità 400 Unità 400F Unità 450F Unità 480 Unità 480F Unità 500 Unità 550F Unità 600F Unità 650F Unità 680F Unità 880 Unity 880F UnityVSA VNXe3200	3.1.17.10229825 4.1.2.9257522 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.3.1.0.6.028 5.4.0.0.5.094 5.4.1.0.5.006

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Volume obiettivo	Implementato	HTTPS	
		Tecnologia	Implementato	HTTPS	tecnologia che causa l'efficienza
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato	HTTPS	Snapshot Capacità utilizzata in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità grezza totale	Implementato	HTTPS	Capacità grezza totale (somma di tutti i dischi nell'array)
		ID pool di archiviazione	Implementato	HTTPS	
		Fornito in modo sottile	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità grezza	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	**Protocollo utilizzato**	**Protocollo di livello di trasporto utilizzato**	**Porte in entrata utilizzate**	**Porte in uscita utilizzate**	**Supporta l'autenticazione**	**Richiede solo credenziali di "sola lettura"**	**Supporta la crittografia**	**Compatibile con firewall (porte statiche)**
CLI VNXe e Unisphere	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

EMC VPLEX

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	**Versioni del firmware**
VPLEX	6.2.0.04.00.07 6.2.0.07.00.02 6.2.1.0.0.519

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
956					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato	HTTP/S	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato	HTTP/S	Snapshot Capacità utilizzata in MB
		Nome	Implementato	HTTP/S	
		Capacità grezza totale	Implementato	HTTP/S	Capacità grezza totale (somma di tutti i dischi nell'array)
		Ridondanza	Implementato	HTTP/S	Livello di ridondanza
		ID pool di archiviazione	Implementato	HTTP/S	
		Fornito in modo sottile	Implementato	HTTP/S	
		UUID	Implementato	HTTP/S	
		Virtuale	Implementato	HTTP/S	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
	Mappa del volume	LUN	Implementato	HTTP/S	Nome del lun backend
		Controllore di protocollo	Implementato	HTTP/S	
		Porto di archiviazione	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	
	Maschera del volume	Iniziatore	Implementato	HTTP/S	
		Controllore di protocollo	Implementato	HTTP/S	
		Porto di archiviazione	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
960					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità grezza	Implementato	SSH	
		Capacità totale	Implementato	SSH	
		IOP totali	Implementato	SSH	
		Chiave	Implementato	SSH	
		Latenza di lettura	Implementato	SSH	
		Latenza totale	Implementato	SSH	
		Latenza di scrittura	Implementato	SSH	
		ID del server	Implementato	SSH	
		Lettura di throughput	Implementato	SSH	
		Portata totale	Implementato	SSH	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	SSH	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
EMC VPLEX CLI	SSH	SSH	22		VERO	VERO	VERO	VERO
API EMC VPLEX	HTTP/HTTPS	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

EMC XtremIO (HTTP)

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
6.2.1 6.3.2 6.3.3 6.4.0 6.4.1 6.4.2	1 Brick e 125 TB 1 Brick e 24 TB 1 Brick e 31 TB 1 Brick e 8 TB 1X10 TB 1X20 TB 1X40 TB 2 Brick e 83 TB 3 Brick e 146 TB 3 Brick e 251 TB 3 Brick e 283 TB 4 Brick e 628 TB 4 Brick e 754 TB 4X20 TB 6X40 TB	4.0.27-1 4.0.31-11 6.3.3-8_X2 6.4.0-36_hotfix_2_X2

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Volume obiettivo	Implementato	HTTPS	
		Tecnologia	Implementato	HTTPS	tecnologia che causa l'efficienza
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato	HTTPS	Snapshot Capacità utilizzata in MB
		Dimensione del disco	Implementato	HTTPS	elenco separato da virgole delle dimensioni del disco (GB)
		Velocità del disco	Implementato	HTTPS	elenco separato da virgole delle velocità del disco (rpm)
		Tipo di disco	Non disponibile	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità grezza totale	Implementato	HTTPS	Capacità grezza totale (somma di tutti i dischi nell'array)
		Ridondanza	Implementato	HTTPS	Livello di ridondanza
		ID pool di archiviazione	Implementato	HTTPS	
		Fornito in modo sottile	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
		UUID	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Controllore di protocollo	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
972					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità grezza	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		Rapporto di blocco parziale	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC XtremIO	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

NetApp E-Series

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
2660 2680 2702 2704 2800B 2804 2806 3000 4000 5486 5488 5504 5564 5600 5700 5700B 6000 7999	08.40.60.01 08.80.00.00 7.84.46.0 8.20.16.0 8.20.27.0 8.20.30.0 8.20.8.0 8.25.14.0 8.25.6.0 8.40.0.1 8.40.20.0 8.40.30.4 8.40.40.0 8.40.50.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.30.5 8.50.0.4 8.51.0.0 8.52.0.0 8.52.0.1 8.53.0.1 8.53.0.4 8.62.0.0 8.62.0.2 8.63.0.2 8.70.0.2 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0 8.75.0.1 8.75.1.0 8.80.0.0 8.80.1.0 8.81.0.3 8.81.1.0 8.81.2.0 8.81.3.0 8.90.0.0

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
978					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato	RMI	Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato	RMI	Snapshot Capacità utilizzata in MB
		Tipo di disco	Non disponibile	RMI	
		Nome	Implementato	RMI	
		Capacità grezza totale	Implementato	RMI	Capacità grezza totale (somma di tutti i dischi nell'array)
		Ridondanza	Implementato	RMI	Livello di ridondanza
		ID pool di archiviazione	Implementato	RMI	
		Fornito in modo sottile	Implementato	RMI	
		Tipo	Spacco	RMI	
		UUID	Implementato	RMI	
		Capacità utilizzata	Implementato	RMI	
		Virtuale	Implementato	RMI	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
		Capacità scritta	Implementato	RMI	Capacità totale scritta su questo volume da un host in MB
	Mappa del volume	LUN	Implementato	RMI	Nome del lun backend
		Porto di archiviazione	Implementato	RMI	
		Tipo	Spacco	RMI	
	Maschera del volume	Iniziatore	Implementato	RMI	
		Porto di archiviazione	Implementato	RMI	
		Tipo	Spacco	RMI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Leggi l'utilizzo	Implementato	RMI	
		Utilizzo totale	Implementato	RMI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Utilizzo Scrivi	Implementato	RMI	
	Volume	Rapporto di lettura della cache	Implementato	RMI	
		Rapporto di hit della cache totale	Implementato	RMI	
		Rapporto di hit della cache in scrittura	Implementato	RMI	
		Capacità grezza	Implementato	RMI	
		Capacità totale	Implementato	RMI	
		Capacità utilizzata	Implementato	RMI	
		Capacità scritta	Implementato	RMI	
		Rapporto di capacità utilizzata	Implementato	RMI	
		CapacityRatio Scritto	Implementato	RMI	
		IOP letti	Implementato	RMI	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	RMI	
		Scrittura IOP	Implementato	RMI	
		Latenza di lettura	Implementato	RMI	
		Latenza totale	Implementato	RMI	
		Latenza di scrittura	Implementato	RMI	
		Lettura di throughput	Implementato	RMI	
		Portata totale	Implementato	RMI	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	RMI	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API SANtricity	RMI	TCP			VERO	VERO	falso	falso

Pure Storage FlashBlade REST

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
Lama di flash Lama di flash//S200	Purezza//FB 4.1.5 Purezza//FB 4.3.0 Purezza//FB 4.3.11 Purezza//FB 4.3.6 Purezza//FB 4.4.3

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità utilizzata istantanea	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità di archiviazione	Implementato	HTTPS	
		Thin Provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
998					

		alla compressione			
		Risparmio totale	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Magazzinaggio	Capacità grezza non riuscita	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Capacità grezza di riserva	Implementato	HTTPS	Capacità grezza dei dischi di riserva (somma di tutti i dischi di riserva)
		Capacità di StoragePools	Implementato	HTTPS	
		Altri IOP	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API FlashBlade di Pure Storage	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Google Cloud Compute

Modelli e versioni supportati da questo raccoglitore dati: Versioni API:

- v1

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Produttore	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		ID	Implementato	HTTPS	
	Informazioni	Descrizione dell'API	Implementato	HTTPS	
		Nome API	Implementato	HTTPS	
		Versione API	Implementato	HTTPS	
		Nome dell'origine dati	Implementato	HTTPS	Informazioni
		Data	Implementato	HTTPS	
		ID dell'originatore	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1004					

		totale			
		Pianifica il tempo di attesa	Implementato	HTTPS	Tempo di attesa per la
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Macchina virtuale	Capacità totale	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Google Compute Platform	HTTPS		443		VERO	VERO	VERO	VERO

Google Cloud Netapp Volumi

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1006					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità dati utilizzata	Implementato	HTTPS	
		Capacità dati	Spacco	HTTPS	capacità

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
		Capacità totale assegnata	Implementato	HTTPS	
		Capacità del disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità grezza per il pool di archiviazione
		Rapporto grezzo/utilizzabile	Implementato	HTTPS	rapporto per convertire dalla capacità utilizzabile alla capacità grezza
			Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1012					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					totale del disco (lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Client	Implementato	HTTPS	
	Disco StoragePool	Spazio di archiviazione degli oggetti utilizzato	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		IOP totali	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Capacità totale dei dati	Implementato	HTTPS	
		Capacità fornita	Implementato	HTTPS	
		Capacità dati utilizzata	Implementato	HTTPS	
		Scrittura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Rapporto di capacità di impegno eccessivo	Implementato	HTTPS	Segnalato come serie temporale

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Google Compute Platform	HTTPS		443		VERO	VERO	VERO	VERO

HDS HCP (HTTPS)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
Piattaforma di contenuti Hitachi	9.6.2.37 9.6.3.33 9.7.2.27 9.7.3.14

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1016					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		assegnata			
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Spacco		HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
prestazione	Magazzinaggio	Capacità grezza non riuscita	Implementato		
		Capacità grezza	Implementato		
		Capacità grezza di riserva	Implementato		Capacità grezza dei dischi di riserva (somma di tutti i dischi di riserva)
		Capacità di StoragePools	Implementato		
		Chiave	Implementato		
		ID del server	Implementato		
	Dati del nodo di archiviazione	Chiave	Implementato		
		ID del server	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		
		Utilizzo totale	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST HDS HCP	HTTPS	HTTPS	9090		VERO	VERO	VERO	VERO

Gestione dispositivi HiCommand

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
7.6.1 8.0 8.7.1 8.7.3 8.7.6 8.8.3	DF850MH DF850S HM800 HM850 P9500 RAID800 VSP5000 XP24000 XP8	0983/AH 0984/BH 0985/BS 0986/AH 0988/HS DKC:60-08-22 DKC:60-08-65 DKC:70-06-43 DKC:80-06-80-00/02 DKC:80-06-91-00/00 DKC:80-06-96-00/00 DKC:83-05-46-60/00 DKC:83-05-50-60/00 DKC:83-05-53-60/00 DKC:88-08-08-60/00 DKC:88-08-10-60/00 DKC:88-08-12-60/00 DKC:88-08-13-60/00 DKC:88-08-13-60/01 DKC:90-08-81-00/00 DKC:90-09-21-00/00 DKC:90-09-23-00/00 DKC:90-09-24-00/00 DKC:90-09-24-00/01 DKC:90-09-25 SVP:60-08-21/00 SVP:60-08-54/00 SVP:70-06-30/00 SVP:80-06-76/02 SVP:80-06-86/00 SVP:80-06-91/00 SVP:83-05-50-60/00 SVP:83-05-54-60/00 SVP:83-05-57-60/00 SVP:88-08-10-60/00 SVP:88-08-12-60/00 SVP:88-08-14-60/00 SVP:88-08-15-60/00 SVP:90-08-81/00 SVP:90-09-21/00 SVP:90-09-23/00 SVP:90-09-24/00 SVP:90-09-25/00

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		archiviazione			
		Fornito in modo sottile	Implementato	API XML HDS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	API XML HDS	
		Capacità utilizzata	Implementato	API XML HDS	
	Mappa del volume	LUN	Implementato	API XML HDS	Nome del lun backend
		Mascheratura obbligatoria	Implementato	API XML HDS	
		Controllore di protocollo	Implementato	API XML HDS	
		Porto di archiviazione	Implementato	API XML HDS	
	Maschera del volume	Iniziatore	Implementato	API XML HDS	
		Controllore di protocollo	Implementato	API XML HDS	
		Porto di archiviazione	Implementato	API XML HDS	
	Membro del volume	Capacità	Implementato	API XML HDS	Snapshot Capacità utilizzata in MB
		Cilindri	Implementato	API XML HDS	
		Nome	Implementato	API XML HDS	
		Rango	Implementato	API XML HDS	
		Capacità grezza totale	Implementato	API XML HDS	Capacità grezza totale (somma di tutti i dischi nell'array)
		ID pool di archiviazione	Implementato	API XML HDS	
		Capacità utilizzata	Implementato	API XML HDS	
	Alias WWN	Alias host	Implementato	API XML HDS	
		Tipo di oggetto	Implementato	API XML HDS	
		Fonte	Implementato	API XML HDS	
		WWN	Implementato	API XML HDS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità utilizzata	Implementato	Esportazione/CLI	
		Rapporto di capacità utilizzata	Implementato	Esportazione/CLI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Chiave	Implementato	Esportazione/CLI	
		ID del server	Implementato	Esportazione/CLI	
		Capacità totale	Implementato	Esportazione/CLI	
		Capacità grezza	Implementato	Esportazione/CLI	
		Capacità utilizzata	Implementato	Esportazione/CLI	
		Rapporto di capacità utilizzata	Implementato	Esportazione/CLI	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Utilità di esportazione (USPV) / SNM CLI (AMS)	Esportazione/CLI				falso	falso	falso	falso
API XML del gestore dispositivi HiCommand	API XML HDS	HTTP/HTTPS	2001		VERO	VERO	VERO	VERO

Centro operativo Hitachi

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
VSP 5100 VSP 5500 VSP 5600 VSP 5600H VSP E1090 VSP E590 VSP E790 VSP E790H VSP F1500 VSP F400 VSP F900 VSP G1000 VSP G1500 VSP G600 VSP G800 VSP G900 XP8	80-06-91-00/00:01-71-03/02 80-06-94-00/00:01-70-03/04 80-06-96-00/00:01-71-03/02 80-06-96-00/00:01-76-03/03 83-05-49-40/01:01-69-03/02 83-05-49-60/01:01-65-03/05 83-05-49-60/01:01-69-03/02 83-05-51-40/00:01-70-03/04 83-05-51-40/00:01-71-03/02 83-05-51-40/00:01-76-03/03 88-08-08-60/00:01-65-03/05 88-08-08-60/00:01-70-03/04 88-08-11-60/00:01-65-03/05 88-08-11-60/00:01-70-03/04 88-08-13-60/00:01-65-03/05 88-08-13-60/01:01-65-03/05 88-08-13-60/01:01-70-03/04 88-08-13-60/01:01-71-03/02 88-08-13-60/01:01-76-03/03 90-08-82-00/00:01-65-03/05 90-08-82:01.70.04 90-09-01-00/01:01-65-03/05 90-09-22-00/00:01-65-03/05 90-09-22-00/00:01-70-03/04 90-09-22-00/00:01-71-03/02 90-09-24-00/01:01-65-03/05 90-09-24-00/01:01-71-03/02 90-09-24-00/01:01-76-03/03 90-09-24:01.65.05 90-09-25-00/00:01-76-03/03 90-09-25:01.70.04 90-09-26-00/00:01-65-03/05 90-09-26-00/00:01-71-03/02 90-09-26-00/00:01-76-03/03 93-07-01-80/00:01-70-03/04 93-07-22-40/00:01-65-03/05 93-07-22-40/00:01-69-03/02 93-07-22-80/00:01-70-03/04 93-07-22-80/00:01-71-03/02 93-07-23-80/00:01-71-03/02 93-07-23-80/01:01-71-03/02 93-07-24-40/00:01-76-03/03 93-07-24-80/00:01-70-03/04 null:null

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1036					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Volume obiettivo	Implementato		
		Tecnologia	Implementato		tecnologia che causa l'efficienza
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato		Snapshot Capacità utilizzata in MB
		Percorso di giunzione	Implementato		
		Nome	Implementato		
		Tipo di protezione	Implementato		
		Capacità grezza totale	Implementato		Capacità grezza totale (somma di tutti i dischi nell'array)
		ID pool di archiviazione	Implementato		
		Fornito in modo sottile	Implementato		
		Tipo	Spacco		
		Capacità utilizzata	Implementato		
		Compressione abilitata	Implementato		
	Mappa del volume	LUN	Implementato		Nome del lun backend
		Mascheratura obbligatoria	Implementato		
		Controllore di protocollo	Implementato		
		Porto di archiviazione	Implementato		
		Tipo	Spacco		
	Maschera del volume	Iniziatore	Implementato		
		Controllore di protocollo	Implementato		
		Porto di archiviazione	Implementato		
		Tipo	Spacco		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Rapporto di lettura della cache	Implementato		
		Rapporto di hit della cache totale	Implementato		
		IOP letti	Implementato		Numero di IOPS di lettura sul disco
		IOP totali	Implementato		
		Scrittura IOP	Implementato		
		Chiave	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Latenza di scrittura	Implementato		
		ID del server	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Hitachi Ops Center	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

HDS HNAS (CLI)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
File 34 G600 G800 HNAS 4060 HNAS 4080 HNAS 4100 N800	14.6.7520.04 14.7.7623.07 14.9.7916.07 15.1.8030.03 15.1.8030.05 15.2.8128.05 15.2.8128.07 15.2.8128.09 15.3.8224.02

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					del dispositivo
		UUID	Implementato	SSH	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Pool di archiviazione	Capacità dati utilizzata	Implementato	SSH	
		Deduplicazione abilitata	Implementato	SSH	La deduplicazione è abilitata sul pool di archiviazione?
		Includi nella capacità DWH	Implementato	SSH	Un modo da ACQ per controllare quali pool di archiviazione sono interessanti in DWH Capacity
		Nome	Implementato	SSH	
		Gruppo di incursione	Implementato	SSH	indica se questo storagePool è un gruppo raid
		Rapporto grezzo/utilizzabile	Implementato	SSH	rapporto per convertire dalla capacità utilizzabile alla capacità grezza
		Capacità utilizzata istantanea	Implementato	SSH	
		ID pool di archiviazione	Implementato	SSH	
		Thin Provisioning supportato	Implementato	SSH	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	SSH	
		Capacità totale utilizzata	Implementato	SSH	Capacità totale in MB
		Tipo	Spacco	SSH	
		Virtuale	Implementato	SSH	Si tratta di un dispositivo di virtualizzazione dell'archiviazione?

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
HDS HNAS CLI	SSH	SSH	22		VERO	VERO	VERO	VERO

Storage HPE Nimble/Alletra 6000

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
v1	5050 6070 AF1000 AF20Q AF40 AF60 AF80 CS1000 CS300 CS3000 CS500 HF20 HF20C HF20H HF40 HF60	5.0.8.0-677726-opz 5.2.1.1100-1027043-opz 5.2.1.400-796142-opz 5.2.1.700-882343-opz 5.2.1.800-930936-opz 6.0.0.400-991061-opz 6.0.0.500-1005932-opz 6.1.1.200-1020304-opz 6.1.1.300-1028597-opz 6.1.2.300-1042680-opz 6.1.2.400-1048557-opz 6.1.2.500-1053701-opz 6.1.2.502-1057650-opz 6.1.2.600-1064273-opz

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1060					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		protocollo			
		Porto di archiviazione	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Alias WWN	Alias host	Implementato	HTTPS	
		Tipo di oggetto	Implementato	HTTPS	
		Fonte	Implementato	HTTPS	
		WWN	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1068					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità grezza	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Risparmio totale sulla compressione	Implementato	HTTPS	
		Risparmio di spazio grazie alla compressione	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST HP Nimble	HTTPS	HTTPS	5392		VERO	falso	VERO	VERO

Huawei OceanStor (REST/HTTPS)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
18800 V5 2600 V3 5310 V5 5500 V3 5500 V5 5800 V3 6800 V3 Dorado 18000 V6 NVMe Dorado 3000 V6 Dorado 5000 V3 Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V500R007C60 Kunpeng V500R007C61 V500R007C71 Kunpeng V600R003C00 V600R005C11 V600R005C26 V600R005C27

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità	Implementato	HTTPS	Snapshot Capacità utilizzata in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità grezza totale	Implementato	HTTPS	Capacità grezza totale (somma di tutti i dischi nell'array)
		Ridondanza	Implementato	HTTPS	Livello di ridondanza
		ID pool di archiviazione	Implementato	HTTPS	
		Fornito in modo sottile	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1082					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Rapporto di lettura della cache	Implementato	HTTPS	
		Rapporto di hit della cache totale	Implementato	HTTPS	
		Rapporto di hit della cache in scrittura	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Huawei OceanStor	HTTPS	HTTPS	8088		VERO	VERO	VERO	VERO
API REST per le prestazioni di Huawei OceanStor	HTTPS	HTTPS	8088		VERO	falso	VERO	VERO

IBM Cleversafe

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1092					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Versione	Implementato	HTTPS	versione del software
Prodotto	**Categoria**	**Caratteristica/attributo gestito**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Pool di archiviazione	Includi nella capacità DWH	Implementato	HTTPS	Un modo da ACQ per controllare quali pool di archiviazione sono interessanti in DWH Capacity
		Nome	Implementato	HTTPS	
		Capacità del disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità grezza per il pool di archiviazione
		Gruppo di incursione	Implementato	HTTPS	indica se questo storagePool è un gruppo raid
		Rapporto grezzo/utilizzabile	Implementato	HTTPS	rapporto per convertire dalla capacità utilizzabile alla capacità grezza
		ID pool di archiviazione	Implementato	HTTPS	
		Thin Provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST IBM Cleversafe	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

IBM DS 8K (DSCLI)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
2107-951 2107-961 2107-993 2107-994 2107-996 2107-A05	- 7.10.1.8 7.6.31.4250 7.7.51.1400 7.9.32.101 7.9.33.132 7.9.33.95 7.9.40.251 7.9.41.65

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

	volume	Controllore di protocollo	Implementato	DSNI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Identificazione	Implementato	DSNI	
	Alias WWN	Alias host	Implementato	DSNI	
		Sistema operativo host	Implementato	DSNI	
		Tipo di oggetto	Implementato	DSNI	
		Fonte	Implementato	DSNI	
		WWN	Implementato	DSNI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1102					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità utilizzata	Implementato	DSNI	
		Rapporto di capacità utilizzata	Implementato	DSNI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Rapporto di lettura della cache	Implementato	DSNI	
		Rapporto di hit della cache totale	Implementato	DSNI	
		Rapporto di hit della cache in scrittura	Implementato	DSNI	
		Capacità grezza	Implementato	DSNI	
		Capacità totale	Implementato	DSNI	
		Capacità utilizzata	Implementato	DSNI	
		Rapporto di capacità utilizzata	Implementato	DSNI	
		IOP letti	Implementato	DSNI	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	DSNI	
		Scrittura IOP	Implementato	DSNI	
		Chiave	Implementato	DSNI	
		Latenza di lettura	Implementato	DSNI	
		Latenza totale	Implementato	DSNI	
		Latenza di scrittura	Implementato	DSNI	
		ID del server	Implementato	DSNI	
		Lettura di throughput	Implementato	DSNI	
		Portata totale	Implementato	DSNI	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	DSNI	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Configurazione guidata origine dati	Inserimento manuale				VERO	VERO	VERO	VERO
IBM DS CLI	DSNI	DSNI			VERO	VERO	VERO	VERO

IBM PowerVM (SSH)

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1108					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		OID del disco virtuale	Implementato	SSH	
		OID della	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attribuito	Stato	Protocollo utilizzato	Informazioni aggiuntive
	Ospite	Conteggio CPU host	Implementato	SSH	
		Memoria installata dall'host	Implementato	SSH	
		Modello host	Implementato	SSH	
		conteggio NIC	Implementato	SSH	
		IP	Implementato	SSH	
		Produttore	Implementato	SSH	
		Nome	Implementato	SSH	
		OID	Implementato	SSH	
		Tipo di piattaforma	Implementato	SSH	
	Informazioni	Nome dell'origine dati	Implementato	SSH	Informazioni
		Data	Implementato	SSH	
		ID dell'originatore	Implementato	SSH	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Accesso SSH alla console di gestione hardware IBM	SSH	SSH	22		VERO	falso	VERO	VERO

IBM SVC (CLI)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
2072-12F 2072-12G 2072-224 2072-24C 2072-24E 2072-24F 2072-24G 2072-2N4 2072-324 2072-3H4 2072-3N2 2072-3N4 2072-92F 2072-92G 2076-124 2076-12F 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2076-AF6 2076- AFF 2077-24F 2077-24G 2077-424 2077-4H4 2078-12F 2078-12G 2078-224 2078-24C 2078-24F 2078-24G 2078-324 2078-424 2078-4H4 2078-92G 2078-AF3 4657-24G 4657-924 4662-12G 4662-24G 4662-6H2 4666-AH8 4666-UH8 4680-24H 4680-2P4 4680-3P4 4680-92H 4983-AH8 9843-AE2 9843-AE3 9846-AG8 9848-AF7 9848-AF8 9848-AG8 9848-UG8 Servizio	1.5.2.7 1.6.1.2 1.6.1.4 1.6.1.5 7.7.1.8 7.8.1.11 7.8.1.12 7.8.1.13 7.8.1.14 7.8.1.16 7.8.1.5 7.8.1.6 7.8.1.7 7.8.1.8 8.2.1.10 8.2.1.8 8.2.1.9 8.3.1.10 8.3.1.2 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.8 8.3.1.9 8.4.0.10 8.4.0.11 8.4.0.13 8.4.0.15 8.4.0.2 8.4.0.5 8.4.0.6 8.4.0.9 8.4.2.0 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.13 8.5.0.14 8.5.0.5 8.5.0.6 8.5.0.7 8.5.0.8 8.5.0.9 8.6.0.0 8.6.0.2 8.6.0.3 8.6.0.4 8.6.0.5 8.7.0.0 8.7.0.1 8.7.0.2 8.7.0.3

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1112					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato	SSH	Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità scritta	Implementato	SSH	Capacità totale scritta su questo volume da un host in MB
		Compressione abilitata	Implementato	SSH	
		Criptato	Implementato	SSH	
	Mappa del volume	LUN	Implementato	SSH	Nome del lun backend
		Controllore di protocollo	Implementato	SSH	
		Porto di archiviazione	Implementato	SSH	
	Maschera del volume	Iniziatore	Implementato	SSH	
		Controllore di protocollo	Implementato	SSH	
		Porto di archiviazione	Implementato	SSH	
		Tipo	Spacco	SSH	
	Alias WWN	Alias host	Implementato	SSH	
		Tipo di oggetto	Implementato	SSH	
		Fonte	Implementato	SSH	
		WWN	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Leggi l'utilizzo	Implementato	SSH	
		Utilizzo totale	Implementato	SSH	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Utilizzo Scrivi	Implementato	SSH	
	Volume	Rapporto di lettura della cache	Implementato	SSH	
		Rapporto di hit della cache totale	Implementato	SSH	
		Rapporto di hit della cache in scrittura	Implementato	SSH	
		Capacità grezza	Implementato	SSH	
		Capacità totale	Implementato	SSH	
		Capacità utilizzata	Implementato	SSH	
		Capacità scritta	Implementato	SSH	
		Rapporto di capacità utilizzata	Implementato	SSH	
		CapacityRatio Scritto	Implementato	SSH	
		IOP letti	Implementato	SSH	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	SSH	
		Scrittura IOP	Implementato	SSH	
		Latenza di lettura	Implementato	SSH	
		Latenza totale	Implementato	SSH	
		Latenza di scrittura	Implementato	SSH	
		Lettura di throughput	Implementato	SSH	
		Portata totale	Implementato	SSH	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	SSH	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
Interfaccia a riga di comando IBM SVC	SSH	SSH	22		VERO	falso	VERO	VERO

IBM XIV e A9000 (XIVCLI)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
A14	10.2.4.e

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1126					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					definita durante le operazioni di creazione o
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Nome	Implementato	XIV CLI	
		ID pool di archiviazione	Implementato	XIV CLI	
		Tipo	Spacco	XIV CLI	
		Tipo di disco	Non disponibile	XIV CLI	
		Gruppo di dischi	Implementato	XIV CLI	Tipo di gruppo di dischi
		Fornito in modo sottile	Implementato	XIV CLI	
		Capacità	Implementato	XIV CLI	Snapshot Capacità utilizzata in MB
		Capacità grezza totale	Implementato	XIV CLI	Capacità grezza totale (somma di tutti i dischi nell'array)
		Capacità utilizzata	Implementato	XIV CLI	
		Ridondanza	Implementato	XIV CLI	Livello di ridondanza
		Compressione abilitata	Implementato	XIV CLI	
	Mappa del volume	LUN	Implementato	XIV CLI	Nome del lun backend
		Controllore di protocollo	Implementato	XIV CLI	
	Maschera del volume	Iniziatore	Implementato	XIV CLI	
		Controllore di protocollo	Implementato	XIV CLI	
	Alias WWN	Fonte	Implementato	XIV CLI	
		Alias host	Implementato	XIV CLI	
		WWN	Implementato	XIV CLI	
		Tipo di oggetto	Implementato	XIV CLI	
		Sistema operativo host	Implementato	XIV CLI	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
IBM DS CLI	DSNI	DSNI			VERO	VERO	VERO	VERO
IBM XIV CLI	XIV CLI	TCP	7778		VERO	falso	VERO	falso

Infinidat Infinibox (HTTP)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
F4303 F6230 F6240	6.0.20.40 6.0.31.0 7.1.14.0 7.1.15.0 7.3.20.90 8.1.0.280

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1132					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		protocollo			
		Porto di archiviazione	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tribù	Spacco	HTTPS	
	Alias WWN	Alias host	Implementato	HTTPS	
		Tipo di oggetto	Implementato	HTTPS	
		Fonte	Implementato	HTTPS	
		WWN	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Infinidat	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Microsoft Azure Compute

Modelli e versioni supportati da questo raccoglitore dati: Versioni API:

- 2018-06-01

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Produttore	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		ID	Implementato	HTTPS	
	Informazioni	Descrizione dell'API	Implementato	HTTPS	
		Nome API	Implementato	HTTPS	
		Versione API	Implementato	HTTPS	
		Nome dell'origine dati	Implementato	HTTPS	Informazioni
		Data	Implementato	HTTPS	
		ID dell'originatore	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1144					

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	macchina virtuale	Capacità totale	Implementato	HTTPS	
		Utilizzo totale della CPU	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		diskIops.totale	Implementato	HTTPS	
		Scrittura IOP su disco	Implementato	HTTPS	
		Lettura della velocità effettiva del disco	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	velocità totale di lettura del disco
		Scrittura della velocità effettiva del disco	Implementato	HTTPS	
		Lettura della velocità effettiva IP	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Throughput IP totale
		ipThroughput.write	Implementato	HTTPS	
	Macchina virtuale	Capacità totale	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Microsoft Azure Compute	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Microsoft Hyper-V

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		OID del disco virtuale	Implementato	WMI	
		OID della macchina	Implementato	WMI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Ospite	Conteggio CPU host	Implementato	WMI	
		Velocità della CPU host	Implementato	WMI	
		Dominio host	Implementato	WMI	
		Memoria installata dall'host	Implementato	WMI	
		Modello host	Implementato	WMI	
		conteggio NIC	Implementato	WMI	
		Velocità NIC	Implementato	WMI	
		IP	Implementato	WMI	
		Produttore	Implementato	WMI	
		Nome	Implementato	WMI	
		OID	Implementato	WMI	
		Tipo di piattaforma	Implementato	WMI	
	Nodo ISCSI	Alias host	Implementato	WMI	
		Nome del nodo	Implementato	WMI	
		OID	Implementato	WMI	
		Tipo	Spacco	WMI	
	Informazioni	Nome dell'origine dati	Implementato	WMI	Informazioni
		Data	Implementato	WMI	
		ID dell'originatore	Implementato	WMI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	macchina virtuale	Capacità totale	Implementato	Gestione WS	
		Capacità utilizzata	Implementato	Gestione WS	
		Rapporto di capacità utilizzata	Implementato	Gestione WS	
		Utilizzo totale della CPU	Implementato	Gestione WS	
		IOP letti	Implementato	Gestione WS	Numero di IOPS di lettura sul disco
		diskIops.totale	Implementato	Gestione WS	
		Scrittura IOP su disco	Implementato	Gestione WS	
		Latenza totale	Implementato	Gestione WS	
		Lettura della velocità effettiva del disco	Implementato	Gestione WS	
		Lettura di throughput	Implementato	Gestione WS	velocità totale di lettura del disco
		Scrittura della velocità effettiva del disco	Implementato	Gestione WS	
		Lettura della velocità effettiva IP	Implementato	Gestione WS	
		Portata totale	Implementato	Gestione WS	Throughput IP totale
		ipThroughput.write	Implementato	Gestione WS	
	Macchina virtuale	Capacità totale	Implementato	Gestione WS	
		Capacità utilizzata	Implementato	Gestione WS	
		Rapporto di capacità utilizzata	Implementato	Gestione WS	
		Chiave	Implementato	Gestione WS	
		ID del server	Implementato	Gestione WS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
PowerShell	Gestione WS	HTTP	5985		VERO	falso	falso	VERO
WMI	WMI	WMI	135		VERO	falso	VERO	VERO

Modalità NetApp 7

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
1.12 1.17 1.19 1.20 1.21	FAS2040 FAS2220 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS3140 FAS3160 FAS3250 FAS3270 FAS6240 FAS6250 FAS8020 FAS8040 FAS8060 N6070 N6240 N6270	8.1.1 7-Mode 8.1.4P9D18 7-Mode 8.2.2 7-Mode 8.2.3 7-Mode 8.2.3P2 7-Mode 8.2.3P3 7-Mode 8.2.4 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.4P6 7-Mode 8.2.5 7-Mode 8.2.5P3 7-Mode 8.2.5P4 7-Mode 8.2.5P5 7-Mode 8.2P3 7-Mode 8.2P4 7-Mode Data ONTAP Release 7.3.3 Data ONTAP Release 8.2.5 7-Mode Data ONTAP Release 8.2.5P1 7-Mode

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

	volume				backend
		Controllore di protocollo	Implementato		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco		
	Maschera del volume	Iniziatore	Implementato		
		Controllore di protocollo	Implementato		
		Porto di archiviazione	Implementato		
		Tipo	Spacco		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					dischi) in MB/s
		Scrittura di throughput	Implementato		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Leggi utilizzo	Implementato		
		Utilizzo totale	Implementato		
		Utilizzo Scrivi	Implementato		
	Volume	Capacità grezza	Implementato		
		Capacità totale	Implementato		
		Capacità utilizzata	Implementato		
		Rapporto di capacità utilizzata	Implementato		
		Lettura densità IO	Implementato		
		Densità IO totale	Implementato		
		Scrivi densità IO	Implementato		
		IOP letti	Implementato		Numero di IOPS di lettura sul disco
		IOP totali	Implementato		
		Scrittura IOP	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Latenza di scrittura	Implementato		
		Rapporto di blocco parziale	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		
		Scrivi in attesa	Implementato		scrittura totale in sospeso

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
NetApp 7 Mode ZAPI	ZAPI	ZAPI			VERO	VERO	VERO	VERO

NetApp E-Series REST

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
2800B 2806 5700	08.71.03.00 08.73.00.00 08.74.02.00 08.75.00.00 08.75.00.01 08.80.00.00 08.81.00.03 08.81.02.00 08.81.03.00 08.90.00.00

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					dispositivo di virtualizzazione dell'archiviazione ?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Criptato	Implementato	HTTPS	
	Volume	Capacità	Implementato	HTTPS	Snapshot Capacità utilizzata in MB
		Tipo di disco	Non disponibile	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità grezza totale	Implementato	HTTPS	Capacità grezza totale (somma di tutti i dischi nell'array)
		Ridondanza	Implementato	HTTPS	Livello di ridondanza
		ID pool di archiviazione	Implementato	HTTPS	
		Fornito in modo sottile	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
		UUID	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
		Criptato	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione	Magazzinaggio	Rapporto di lettura della cache	Implementato	HTTPS	
		Rapporto di hit della cache totale	Implementato	HTTPS	
		Rapporto di hit della cache in scrittura	Implementato	HTTPS	
		Capacità grezza non riuscita	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Capacità grezza di riserva	Implementato	HTTPS	Capacità grezza dei dischi di riserva (somma di tutti i dischi di riserva)
		Capacità di StoragePools	Implementato	HTTPS	
		Altri IOP	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST NetApp E-Series	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Amazon FSx for NetApp ONTAP

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
FSx per ONTAP	Data ONTAP

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1190					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		protocollo			
		Porto di archiviazione	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		impegno eccessivo			
		Capacità	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità riservata snapshot	Implementato	HTTPS	
	Macchina Virtuale	Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API ONTAP NetApp	HTTP/HTTPS	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

NetApp Clustered Data ONTAP 8.1.1+

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
AFF-A150 AFF-A1K AFF-A20 AFF-A200 AFF-A220 AFF-A300 AFF-A320 AFF-A400 AFF-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C60 AFF-C80 AFF-C800 AFF AFF8040 AFF8060 AFF8080 ASA-A250 ASA-A400 ASA-A800 ASA-A900 ASA-C250 ASA-C400 ASA-C800 CDvM100 CDvM200 DM5000H DM7100F FAS2240-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS2820 FAS3220 FAS3250 FAS3270 FAS500f FAS6210 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• 8.2.3P4 • 8.2.3P5 • 8.3.1P2 • 8.3.2 • 8.3.2P12 • 8.3.2P5 • 9.0.0 • 9.1.0 • 9.1.0P1 • 9.1.0P11 • 9.1.0P15 • 9.1.0P17 • 9.1.0P19 • 9.1.0P2 • 9.1.0P20 • 9.1.0P3 • 9.1.0P6 • 9.1.0P7 • 9.1.0P8 • 9.1.0P9 • 9.10.0 • 9.10.1 • 9.10.1P1 • 9.10.1P10 • 9.10.1P11 • 9.10.1P12 • 9.10.1P13 • 9.10.1P14 • 9.10.1P15 • 9.10.1P16 • 9.10.1P17 • 9.10.1P18 • 9.10.1P19 • 9.10.1P2 • 9.10.1P20 • 9.10.1P3 9.10.1P4 9.10.1P5

Prodotti supportati da questo raccoglitore dati:

-
- 9.10.1P6
- 9.10.1P7
- 9.10.1P8
- 9.10.1P9
- 9.11.0P1
- 9.11.1
- 9.11.1P1
- 9.11.1P10
- 9.11.1P11
- 9.11.1P12
- 9.11.1P13
- 9.11.1P14
- 9.11.1P15
- 9.11.1P16
- 9.11.1P17
- 9.11.1P18
- 9.11.1P2
- 9.11.1P3
- 9.11.1P4
- 9.11.1P5
- 9.11.1P6
- 9.11.1P7
- 9.11.1P8
- 9.11.1P9
- 9.12.1
- 9.12.1P1
- 9.12.1P10
- 9.12.1P11
- 9.12.1P12
- 9.12.1P13
- 9.12.1P14
- 9.12.1P15
- 9.12.1P16
- 9.12.1P17
- 9.12.1P2
- 9.12.1P3

9.12.1P4

9.12.1P5

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione			• 9.12.1P7 • 9.12.1P8 • 9.12.1P9 • 9.13.0 • 9.13.0P1 • 9.13.0P3 • 9.13.1 • 9.13.1D1 • 9.13.1P1 • 9.13.1P10 • 9.13.1P11 • 9.13.1P12 • 9.13.1P13 • 9.13.1P14 • 9.13.1P2 • 9.13.1P3 • 9.13.1P4 • 9.13.1P5 • 9.13.1P6 • 9.13.1P7 • 9.13.1P8 • 9.13.1P9 • 9.14.0 • 9.14.0P1 • 9.14.0P2 • 9.14.1 • 9.14.1P1 • 9.14.1P10 • 9.14.1P11 • 9.14.1P2 • 9.14.1P4 • 9.14.1P5 • 9.14.1P6 • 9.14.1P7 • 9.14.1P8 9.14.1P8D5 9.14.1P9		
1216					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
			• 9.15.0P2 • 9.15.1 • 9.15.1P1 • 9.15.1P2 • 9.15.1P2D2 • 9.15.1P3 • 9.15.1P4 • 9.15.1P5 • 9.15.1P6 • 9.15.1P7 • 9.15.1P7D4 • 9.15.1P8 • 9.16.1 • 9.16.1P1 • 9.17.1 • 9.2.0P3 • 9.2.0P4 • 9.3.0P15 • 9.3.0P18 • 9.3.0P20 • 9.3.0P21 • 9.3.0P6 • 9.3.0P7 • 9.3.0P8 • 9.4.0 • 9.4.0P2 • 9.4.0P5 • 9.5.0 • 9.5.0P1 • 9.5.0P10 • 9.5.0P14 • 9.5.0P16 • 9.5.0P17 • 9.5.0P18 • 9.5.0P19 9.5.0P2 9.5.0P3		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
			• 9.5.0P7 • 9.5.0P9 • 9.6.0 • 9.6.0P11 • 9.6.0P18 • 9.6.0P2 • 9.6.0P3 • 9.6.0P5 • 9.7.0 • 9.7.0P10 • 9.7.0P11 • 9.7.0P12 • 9.7.0P13 • 9.7.0P14 • 9.7.0P15 • 9.7.0P16 • 9.7.0P17 • 9.7.0P18 • 9.7.0P19 • 9.7.0P20 • 9.7.0P21 • 9.7.0P22 • 9.7.0P23 • 9.7.0P4 • 9.7.0P5 • 9.7.0P6 • 9.7.0P7 • 9.7.0P8 • 9.7.0P9 • 9.8.0 • 9.8.0P1 • 9.8.0P10 • 9.8.0P11 • 9.8.0P12 • 9.8.0P13 9.8.0P14 9.8.0P15		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
			• 9.8.0P17 • 9.8.0P18 • 9.8.0P19 • 9.8.0P2 • 9.8.0P20 • 9.8.0P21 • 9.8.0P3 • 9.8.0P4 • 9.8.0P6 • 9.8.0P7 • 9.8.0P8 • 9.8.0P9 • 9,0 • 9,1 • 9.9.1P10 • 9.9.1P11 • 9.9.1P12 • 9.9.1P13 • 9.9.1P14 • 9.9.1P15 • 9.9.1P16 • 9.9.1P17 • 9.9.1P18 • 9.9.1P19 • 9.9.1P2 • 9.9.1P20 • 9.9.1P3 • 9.9.1P6 • 9.9.1P7 • 9.9.1P9		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					dell'archiviazione ?
		Criptato	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Limite Qos IOPS	Implementato	HTTPS	
		Limite Qos MBPS	Implementato	HTTPS	
		Limite Qos grezzo	Implementato	HTTPS	
		QoS - Politica	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
		Capacità utilizzata	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Thick server	Implementato	HTTPS	
	Volume	Capacità grezza	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Lettura densità IO	Implementato	HTTPS	
		Densità IO totale	Implementato	HTTPS	
		Scrivi densità IO	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		Rapporto di blocco parziale	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API ONTAP NetApp	HTTP/HTTPS	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

ASA

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
ASA-A1K ASA-A20 ASA-A90	NetApp Release 9.16.1: Sab 18 Gen 19:31:15 UTC 2025 NetApp Release 9.16.1RC1: Lun 04 Nov 10:39:46 UTC 2024

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		protocollo			
		Porto di archiviazione	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
prestazione	Disco	IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	
		Leggi l'utilizzo	Implementato	HTTPS	
		Utilizzo totale	Implementato	HTTPS	
		Utilizzo Scrivi	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API ASA NetApp	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

NetApp ONTAP REST

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
AFF-A150 AFF-A220 AFF-A250 AFF-A300 AFF -A400 AFF-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 AFF-A250 ASA-A400 ASA-A800 ASA-C250 ASA-C800 ASA FAS2720 FAS2750 FAS2820 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• NetApp Release 9.14.1P10: giovedì 28 novembre 12:32:16 UTC 2024 • NetApp Release 9.14.1P11: mercoledì 22 gennaio 11:55:28 UTC 2025 • NetApp Release 9.14.1P1: giovedì 15 febbraio 00:45:21 UTC 2024 • NetApp Release 9.14.1P4: giovedì 18 aprile 15:59:10 UTC 2024 • NetApp Release 9.14.1P5: sabato 18 maggio 19:42:16 UTC 2024 • NetApp Release 9.14.1P6: martedì 18 giugno 16:11:44 UTC 2024 • NetApp Release 9.14.1P7: giovedì 1 agosto 2024, ore 03:07:44 UTC • NetApp Release 9.14.1P8: ven 13 set 07:12:27 UTC 2024 • NetApp Release 9.14.1P9: lunedì 21 ottobre 18:04:05 UTC 2024 • NetApp Release 9.15.1: giovedì 4 luglio 2024, ore 12:21:07 UTC • NetApp Release 9.15.1P1: martedì 30 luglio 05:15:49 UTC 2024 • NetApp Release 9.15.1P2: martedì 27 agosto 16:35:16 UTC 2024 • NetApp Release 9.15.1P3: mercoledì 25 settembre 2024, ore 22:33:44 UTC • NetApp Release 9.15.1P4: domenica 27 ottobre 2024, ore 20:15:53 UTC • NetApp Release 9.15.1P5: domenica 24 novembre 16:31:37 UTC 2024 • NetApp Release 9.15.1P6: mercoledì 4 dicembre 2024, ore 01:42:39 UTC • NetApp Release 9.15.1P7: Sab 18 Gen 2025 21:34:02 UTC • NetApp Release 9.15.1RC2: lunedì 24 giugno 2024, ore 04:49:55 UTC • NetApp Release 9.16.1: Sab 18 Gen 19:31:15 UTC 2025 • NetApp Release 9.16.1P1: ven 14 feb 03:53:50 UTC 2025 • NetApp Release 9.16.1RC1: lunedì 4 novembre 2024, ore 10:39:46 UTC • NetApp rilascia Clawhammer__9.14.1: sabato 18 maggio 09:23:49 UTC 2024 • NetApp rilascia Cloudstream__9.16.1: lunedì 4 novembre 2024, ore 05:51:46 UTC

Prodotti supportati da questo raccoglitore dati:

-
- NetApp rilascia Cloudstream__9.16.1: giovedì 13 marzo 2025, ore 20:55:54 UTC
- NetApp rilascia Electricjellyfish__9.17.1: lunedì 3 marzo 2025, ore 05:57:49 UTC
- NetApp rilascia Electricjellyfish__9.17.1: domenica 9 marzo 2025, ore 05:56:14 UTC
- NetApp rilascia Electricjellyfish__9.17.1: domenica 16 marzo 2025, ore 04:54:53 UTC
- NetApp rilascia Electricjellyfish__9.17.1: martedì 28 gennaio 11:48:14 UTC 2025
- NetApp rilascia Electricjellyfish__9.17.1: martedì 18 marzo 2025, ore 04:59:54 UTC
- NetApp rilascia Electricjellyfish__9.17.1: mercoledì 12 marzo 2025, ore 04:42:03 UTC
- NetApp rilascia Mightysquirrel__9.15.1: venerdì 24 maggio 05:03:10 UTC 2024
- NetApp rilascia Mightysquirrel__9.15.1: sabato 18 gennaio 11:39:42 UTC 2025
- NetApp rilascia Tropicallightning__9.18.0: ven 21 feb 14:02:58 UTC 2025
- NetApp rilascia Tropicallightning__9.18.0: lunedì 17 febbraio 08:18:14 UTC 2025
- NetApp rilascia Tropicallightning__9.18.0: giovedì 20 febbraio 2025, ore 08:11:55 UTC
- NetApp rilascia Tropicallightning__9.18.0: giovedì 27 febbraio 2025, ore 04:15:40 UTC
- NetApp rilascia Tropicallightning__9.18.0: martedì 18 febbraio 14:00:54 UTC 2025
- NetApp rilascia Tropicallightning__9.18.0: mercoledì 26 febbraio 08:19:21 UTC 2025
- NetApp rilascia Tropicallightning__9.18.0: mercoledì 29 gennaio 2025, ore 08:34:06 UTC

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					dispositivo di virtualizzazione dell'archiviazione ?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Criptato	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		ID del server	Implementato	HTTPS	
		Capacità	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
		Capacità utilizzata istantanea	Implementato	HTTPS	
		Rapporto di capacità utilizzata istantanea	Implementato	HTTPS	Segnalato come serie temporale

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST ONTAP NetApp	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

NetApp SolidFire 8.1+

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
H410S-2 H610S-2 H610S-4 SF19210 SF2405 SF4805 SF9605 SF9608 H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 SF19210 SF38410 SF4805 SF9605 SF9608	11.1.0.72 11.7.0.76 12.0.0.333 12.2.0.777 12.3.0.958 12.3.1.103 12.3.1.165 12.3.2.3 12.5.0.897 12.7.0.380

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1288					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Limite Qos IOPS	Implementato	HTTPS	
		QoS Min IOPS	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		QoS Politica	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Mascheratura obbligatoria	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1296					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Utilizzo totale	Implementato	HTTPS	
	Volume	Capacità grezza	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Risparmio totale sulla compressione	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		Rapporto di blocco parziale	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	
		Utilizzo totale	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST SolidFire	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

NetApp StorageGRID (HTTPS)

Modelli e versioni supportati da questo raccoglitore dati:

Versioni API	Modelli	Versioni del firmware
3.2 3.3 3.4 3.5 4.0 4.1	Scala Web	11.4.0 11.5.0.11 11.5.0.6 11.5.0.7 11.5.0.9 11.6.0 11.6.0.10 11.6.0.11 11.6.0.12 11.6.0.13 11.6.0.14 11.6.0.15 11.6.0.16 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0 11.7.0.11 11.7.0.12 11.7.0.13 11.7.0.3 11.7.0.4 11.7.0.5 11.7.0.6 11.7.0.8 11.7.0.9 11.8.0 11.8.0.1 11.8.0.2 11.8.0.3 11.8.0.5 11.8.0.6 11.8.0.7 11.8.0.8 11.8.0.9 11.9.0 11.9.0.1 11.9.0.2 11.9.0.3 11.9.0.4

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Utilizzo della capacità del nodo Metadati utilizzati in MB	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Nome del sito	Implementato	HTTPS	
	Pool di archiviazione	Includi nella capacità DWH	Implementato	HTTPS	Un modo da ACQ per controllare quali pool di archiviazione sono interessanti in DWH Capacity
		Nome	Implementato	HTTPS	
		Capacità del disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità grezza per il pool di archiviazione
		Gruppo di incursione	Implementato	HTTPS	indica se questo storagePool è un gruppo raid
		Rapporto grezzo/utilizzabile	Implementato	HTTPS	rapporto per convertire dalla capacità utilizzabile alla capacità grezza
		ID pool di archiviazione	Implementato	HTTPS	
		Thin Provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Dati del nodo di archiviazione	Chiave	Implementato		
		Metadati consentiti per l'utilizzo della capacità del nodo	Implementato		
		Utilizzo totale della capacità del nodo	Implementato		
		Utilizzo della capacità del nodo utilizzabile	Implementato		
		Utilizzo della capacità del nodo utilizzato	Implementato		
		Metadati utilizzati per l'utilizzo della capacità del nodo	Implementato		
		ID del server	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		
	Disco StoragePool	Capacità fornita	Implementato		
		Capacità grezza	Implementato		
		Capacità totale	Implementato		
		Capacità utilizzata	Implementato		
		Rapporto di capacità di impegno eccessivo	Implementato		Segnalato come serie temporale
		Rapporto di capacità utilizzata	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di StorageGrid	HTTPS	HTTPS	443		VERO	falso	VERO	VERO

Archiviazione Nutanix (REST)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
NX-3170-G7 NX-8155-G7 HPE DX380 12LFF G11 HPE DX380-24 G10 HPE DX385-12 Gen10 Plus NX-3060-G6 NX-3060-G7 NX-3060-G8 NX-3155G-G7 NX-3155G-G8 NX-3170-G6 NX-8035-G8 NX-8150-G7 NX-8150-G8 NX-8155-G8 XF3070 XF8050-Core	5.20.1.1 6.10 6.10.1 6.5.3.7 6.5.4 6.5.5.1 6.5.5.7 6.5.6 6.5.6.5 6.5.6.6 6.5.6.7 6.7.1.6 7.0

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					livello del volume sopra di esso
Prodotto	**Categoria**	**Capacità totale/attribuita assegnata**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
	Volume	Capacità	Implementato	HTTPS	Snapshot Capacità utilizzata in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		ID Qtree	Implementato	HTTPS	ID univoco del qtree
		Capacità grezza totale	Implementato	HTTPS	Capacità grezza totale (somma di tutti i dischi nell'array)
		Ridondanza	Implementato	HTTPS	Livello di ridondanza
		ID pool di archiviazione	Implementato	HTTPS	
		Fornito in modo sottile	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun backend
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Maschera del volume	Iniziatore	Implementato	HTTPS	
		Controllore di protocollo	Implementato	HTTPS	
		Porto di archiviazione	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1324					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					(lettura e scrittura su tutti i dischi) in MB/s
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Disco StoragePool	IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	
	Volume	Latenza totale	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		Latenza di lettura	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Scrittura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		IOP totali	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Nutanix	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

OpenStack (API REST / SSH)

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1328					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		IP	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		OID	Implementato	HTTPS	
	Nodo ISCSI	Alias host	Implementato	HTTPS	
		Nome del nodo	Implementato	HTTPS	
		OID	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
	Informazioni	Nome dell'origine dati	Implementato	HTTPS	Informazioni
		Data	Implementato	HTTPS	
		ID dell'originatore	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	
prestazione	Ospite	Utilizzo totale della CPU	Implementato		
		Chiave	Implementato		
		Utilizzo totale della memoria	Implementato		
		ID del server	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di OpenStack	HTTPS	HTTPS	443		VERO	falso	VERO	VERO
OpenStack SSH	SSH	SSH	22		VERO	falso	VERO	VERO

Oracle ZFS (HTTPS)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
Archiviazione Sun ZFS 7120 Archiviazione Sun ZFS 7320 Archiviazione Sun ZFS 7330 Archiviazione Sun ZFS 7335 Archiviazione Sun ZFS 7350 Archiviazione Sun ZFS 7370 Archiviazione Sun ZFS 7390 Archiviazione Sun ZFS 7420	1-1.1 1-1.2 1-1.3 1-1.34 1-1.4 2013.06.05.6.12 2013.06.05.6.15 2013.06.05.7.21 2013.06.05.7.24 2013.06.05.7.25 2013.06.05.7.26 2013.06.05.7.29 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.37 2013.06.05.8.44 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.56 2013.06.05.8.6 2013.06.05.8.61 2013.06.05.8.65 2013.06.05.8.7 2013.06.05.8.72 2013.06.05.8.74 2013.06.05.8.76

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Virtuale	Implementato	HTTP/S	Si tratta di un dispositivo di virtualizzazione
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Mappa del volume	LUN	Implementato	HTTP/S	Nome del lun backend
		Mascheratura obbligatoria	Implementato	HTTP/S	
		Controllore di protocollo	Implementato	HTTP/S	
		Porto di archiviazione	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	
	Maschera del volume	Iniziatore	Implementato	HTTP/S	
		Controllore di protocollo	Implementato	HTTP/S	
		Porto di archiviazione	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità di StoragePools	Implementato		
		Chiave	Implementato		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		ID del server	Implementato		
	Nodo di archiviazione	IOP letti	Implementato		Numero di IOPS di lettura sul disco
		Scrittura IOP	Implementato		
		IOP totali	Implementato		
		Rapporto di hit della cache totale	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Utilizzo totale	Implementato		
		Scrittura di throughput	Implementato		
		Lettura di throughput	Implementato		
	Dati del nodo di archiviazione	Rapporto di hit della cache totale	Implementato		
		IOP letti	Implementato		Numero di IOPS di lettura sul disco
		IOP totali	Implementato		
		Scrittura IOP	Implementato		
		Chiave	Implementato		
		ID del server	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		
		Utilizzo totale	Implementato		
	Disco StoragePool	IOP totali	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Oracle ZFS	HTTP/HTTPS	HTTP/HTTPS	215		VERO	VERO	VERO	VERO

Pure Storage FlashArray (HTTP)

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
DFSC1 FA-450 FA-C40R3 FA-C50R4 FA-C60 FA-C60R3 FA-C70R4 FA-C90R4 FA-X10R2 FA-X10R3 FA-X20R2 FA-X20R3 FA-X20R4 FA-X50R2 FA-X50R3 FA-X50R4 FA-X70R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4 FA-XL130 FA-XL170 FA-m20 FA-m20r2 FA-m50 FA-m70 FA-m70r2 OSSIGENO	5.3.14 5.3.20 6.1.10 6.1.14 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.2.10 6.3.10 6.3.11 6.3.12 6.3.13 6.3.14 6.3.15 6.3.16 6.3.17 6.3.18 6.3.3 6.3.6 6.3.7 6.3.9 6.4.10 6.4.2 6.4.3 6.4.7 6.4.8 6.4.9 6.5.0 6.5.1 6.5.2 6.5.3 6.5.4 6.5.5 6.5.6 6.5.7 6.5.8 6.5.9 6.6.10 6.6.11 6.6.5 6.6.6 6.6.7 6.7.0 6.7.1 6.8.1 6.8.2 6.8.3

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					scritta su questo volume da un host in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Mappa del volume	LUN	Implementato	HTTP/S	Nome del lun backend
		Controllore di protocollo	Implementato	HTTP/S	
		Porto di archiviazione	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	
	Maschera del volume	Iniziatore	Implementato	HTTP/S	
		Controllore di protocollo	Implementato	HTTP/S	
		Porto di archiviazione	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	
	Alias WWN	Alias host	Implementato	HTTP/S	
		Tipo di oggetto	Implementato	HTTP/S	
		Fonte	Implementato	HTTP/S	
		WWN	Implementato	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		istantanea			
		Rapporto di capacità	Implementato		Segnalato come serie temporale
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
	Volume	Capacità grezza	Implementato		
		Capacità totale	Implementato		
		Capacità utilizzata	Implementato		
		Rapporto di capacità utilizzata	Implementato		
		IOP letti	Implementato		Numero di IOPS di lettura sul disco
		IOP totali	Implementato		
		Scrittura IOP	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Latenza di scrittura	Implementato		
		Lettura di throughput	Implementato		
		Portata totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato		

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Pure Storage	HTTP/HTTPS	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

Red Hat RHV (REST)

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1360					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		OID del disco virtuale	Implementato	HTTP/S	
		OID della macchina	Implementato	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
	Ospite	Conteggio CPU host	Implementato	HTTP/S	
		Velocità della CPU host	Implementato	HTTP/S	
		Memoria installata dall'host	Implementato	HTTP/S	
		Modello host	Implementato	HTTP/S	
		conteggio NIC	Implementato	HTTP/S	
		Velocità NIC	Implementato	HTTP/S	
		IP	Implementato	HTTP/S	
		Produttore	Implementato	HTTP/S	
		Nome	Implementato	HTTP/S	
		OID	Implementato	HTTP/S	
		Tipo di piattaforma	Implementato	HTTP/S	
	Nodo ISCSI	Nome del nodo	Implementato	HTTP/S	
		OID	Implementato	HTTP/S	
		Tipo	Spacco	HTTP/S	
	Informazioni	Nome dell'origine dati	Implementato	HTTP/S	Informazioni
		Data	Implementato	HTTP/S	
		ID dell'originatore	Implementato	HTTP/S	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Red Hat RHEV	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Rubrik Storage

Modelli e versioni supportati da questo raccoglitore dati: Versioni firmware:

- 8.1.3-p12-25506
- 8.1.3-p13-25544
- 8.1.3-p2-24912
- 9.0.3-p10-25744
- 9.0.3-p5-25595
- 9.0.3-p6-25611
- 9.1.1-27527
- 9.1.2-27824
- 9.1.2-p1-27870
- 9.1.2-p1-27870_HP1473894
- 9.1.3-p1-28075
- 9.1.3-p8-28434
- 9.2.2-p1-29213
- 9.2.3-29313
- 9.2.3-p1-29368

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		assegnata			
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
		Percentuale di capacità effettiva utilizzata	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1370					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

					dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Utilizzo totale	Implementato	HTTPS	
	Disco StoragePool	IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		Scrittura IOP	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Scrittura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		IOP totali	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Altra capacità utilizzata	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Rapporto di capacità utilizzata	Implementato	HTTPS	
		Capacità dati utilizzata	Implementato	HTTPS	
		Capacità utilizzata istantanea	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Rubrik Storage	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

VAST DataStore

Modelli e versioni supportati da questo raccoglitore dati:

Modelli	Versioni del firmware
VA2437096 Dati VAST	Versione build: release-5.0.0-sp24-1389206 Versione build: release-5.0.0-sp24-1389206 Versione build: release-5.0.0-sp70-1532643 Versione build: release-5.1.0-sp50-1578267 Versione build: release-5.1.0-sp51-hf3-1643358 Versione build: release-5.1.0-sp56-1630237 Versione build: release-5.1.0-sp56-hf10-1682647 Versione build: release-5.1.0-sp56-hf14-1700467 Versione di sistema: 5.0.0.94 Versione di sistema: 5.0.0.133 Versione di sistema: 5.0.0.94 Versione di sistema: 5.1.0.210 Versione del sistema: 5.1.0.231

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità utilizzata istantanea	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Capacità di archiviazione	Implementato	HTTPS	
		Thin Provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il provisioning sottile per il livello del volume sopra di esso
		Capacità totale assegnata	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Spacco	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo di virtualizzazione dell'archiviazione ?
		Criptato	Implementato	HTTPS	
	Macchina virtuale di archiviazione	Capacità allocata (MB)	Implementato	HTTPS	Capacità allocata degli snapshot
		Commento	Implementato	HTTPS	
		Chiave guida	Implementato	HTTPS	Chiave univoca globale della macchina virtuale di archiviazione
		Nome	Implementato	HTTPS	
		Tipo	Spacco	HTTPS	
		UUID	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
	Riferimento al volume interno della macchina virtuale	ID volume interno	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione	Magazzinaggio	Capacità grezza non riuscita	Implementato	HTTPS	
		Capacità grezza	Implementato	HTTPS	
		Capacità grezza di riserva	Implementato	HTTPS	Capacità grezza dei dischi di riserva (somma di tutti i dischi di riserva)
		Capacità di StoragePools	Implementato	HTTPS	
		Lettura densità IO	Implementato	HTTPS	
		Densità IO totale	Implementato	HTTPS	
		Scrivi densità IO	Implementato	HTTPS	
		Altri IOP	Implementato	HTTPS	
		IOP letti	Implementato	HTTPS	Numero di IOPS di lettura sul disco
		IOP totali	Implementato	HTTPS	
		Scrittura IOP	Implementato	HTTPS	
		Chiave	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Latenza di scrittura	Implementato	HTTPS	
		ID del server	Implementato	HTTPS	
		Lettura di throughput	Implementato	HTTPS	
		Portata totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s
		Scrittura di throughput	Implementato	HTTPS	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API VAST DataStore	HTTPS	HTTPS	443		VERO	VERO	VERO	VERO

Centro virtuale NetApp HCI

Modelli e versioni supportati da questo raccoglitore dati: Versioni API:

- VMware vCenter Server 6.7.0 build-10244857
- VMware vCenter Server 7.0.3 build-20395099

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					
1386					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Nome del nodo	Implementato	Servizi Web	
		OID	Implementato	Servizi Web	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	Servizi Web	
	Informazioni	Descrizione dell'API	Implementato	Servizi Web	
		Nome API	Implementato	Servizi Web	
		Versione API	Implementato	Servizi Web	
		Nome API client	Implementato	Servizi Web	
		Versione API client	Implementato	Servizi Web	
		Nome dell'origine dati	Implementato	Servizi Web	Informazioni
		Data	Implementato	Servizi Web	
		ID dell'originatore	Implementato	Servizi Web	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Scrittura della velocità effettiva del disco	Implementato	Servizi Web	
Prodotto	**Categoria**	**Utilizzo totale/attivato CPU**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Utilizzo totale/attivato CPU	Implementato	Servizi Web	
		Pianifica il tempo di attesa	Implementato	Servizi Web	Tempo di attesa per la programmazione in percentuale
		diskIops.totale	Implementato	Servizi Web	
		Tasso di swap totale	Implementato	Servizi Web	
		Lettura di throughput	Implementato	Servizi Web	velocità totale di lettura del disco

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST VMware	Servizi Web	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

VMware Cloud su AWS

Modelli e versioni supportati da questo raccoglitore dati: Versioni API:

- VMware vCenter Server 7.0.3 build-21477706
- VMware vCenter Server 7.0.3 build-24322018
- VMware vCenter Server 8.0.0 build-22877852
- VMware vCenter Server 8.0.1 build-22161730
- VMware vCenter Server 8.0.1 build-23525738
- VMware vCenter Server 8.0.3 build-24322831

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Capacità fornita	Implementato	Servizi Web	
		Capacità utilizzata	Implementato	Servizi Web	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		UUID	Implementato	Servizi Web	
	Disco VirtualMachine	OID	Implementato	Servizi Web	
		OID del disco virtuale	Implementato	Servizi Web	
		OID della macchina virtuale	Implementato	Servizi Web	
	Ospite	Conteggio CPU host	Implementato	Servizi Web	
		Velocità della CPU host	Implementato	Servizi Web	
		Dominio host	Implementato	Servizi Web	
		Memoria installata dall'host	Implementato	Servizi Web	
		Modello host	Implementato	Servizi Web	
		conteggio NIC	Implementato	Servizi Web	
		Velocità NIC	Implementato	Servizi Web	
		IP	Implementato	Servizi Web	
		Produttore	Implementato	Servizi Web	
		Nome	Implementato	Servizi Web	
		OID	Implementato	Servizi Web	
		Tipo di piattaforma	Implementato	Servizi Web	
	Informazioni	Descrizione dell'API	Implementato	Servizi Web	
		Nome API	Implementato	Servizi Web	
		Versione API	Implementato	Servizi Web	
		Nome API client	Implementato	Servizi Web	
		Versione API client	Implementato	Servizi Web	
		Nome dell'origine dati	Implementato	Servizi Web	Informazioni
		Data	Implementato	Servizi Web	
		ID dell'originatore	Implementato	Servizi Web	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione	Ospite	Utilizzo totale della CPU	Implementato	Servizi Web	
		IOP letti	Implementato	Servizi Web	Numero di IOPS di lettura sul disco
		diskIops.totale	Implementato	Servizi Web	
		Scrittura IOP su disco	Implementato	Servizi Web	
		Latenza di lettura	Implementato	Servizi Web	
		Latenza totale	Implementato	Servizi Web	
		Latenza di scrittura	Implementato	Servizi Web	
		Lettura della velocità effettiva del disco	Implementato	Servizi Web	
		Lettura di throughput	Implementato	Servizi Web	velocità totale di lettura del disco
		Scrittura della velocità effettiva del disco	Implementato	Servizi Web	
		Lettura della velocità effettiva IP	Implementato	Servizi Web	
		Portata totale	Implementato	Servizi Web	Throughput IP totale
		ipThroughput.write	Implementato	Servizi Web	
		Chiave	Implementato	Servizi Web	
		Utilizzo totale della memoria	Implementato	Servizi Web	
		ID del server	Implementato	Servizi Web	
		swapRate.inRate	Implementato	Servizi Web	
		Tasso di swap	Implementato	Servizi Web	
		Tasso di swap totale	Implementato	Servizi Web	

API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST VMware	Servizi Web	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

VMware vSphere (servizi Web)

Modelli e versioni supportati da questo raccoglitore dati: Versioni API:

- VMware ESXi 6.0.0 build-10474991
- VMware ESXi 6.0.0 build-10719132
- VMware ESXi 6.0.0 build-13635687
- VMware ESXi 6.0.0 build-2494585
- VMware ESXi 6.0.0 build-3620759
- VMware ESXi 6.0.0 build-5050593
- VMware ESXi 6.0.0 build-5224934
- VMware ESXi 6.0.0 build-9239799
- VMware ESXi 6.5.0 build-5310538
- VMware ESXi 7.0.3 build-20036589
- VMware ESXi 7.0.3 build-20328353
- VMware ESXi 8.0.0 build-21203435
- VMware ESXi 8.0.1 build-21495797
- VMware vCenter Server 5.0.0 build-623373
- VMware vCenter Server 5.5.0 build-1750787
- VMware vCenter Server 5.5.0 build-2442329
- VMware vCenter Server 5.5.0 build-3252642
- VMware vCenter Server 5.5.0 build-6516310
- VMware vCenter Server 5.5.0 build-9911218
- VMware vCenter Server 6.0.0 build-13638472
- VMware vCenter Server 6.0.0 build-14510545
- VMware vCenter Server 6.0.0 build-2776511
- VMware vCenter Server 6.0.0 build-3634793
- VMware vCenter Server 6.0.0 build-5183551
- VMware vCenter Server 6.0.0 build-9313458
- VMware vCenter Server 6.5.0 build-10964411
- VMware vCenter Server 6.5.0 build-12863991
- VMware vCenter Server 6.5.0 build-15259038

- VMware vCenter Server 6.5.0 build-17994927
- VMware vCenter Server 6.5.0 build-18499837
- VMware vCenter Server 6.5.0 build-18711281
- VMware vCenter Server 6.5.0 build-20510539
- VMware vCenter Server 6.5.0 build-22499743
- VMware vCenter Server 6.5.0 build-5973321
- VMware vCenter Server 6.7.0 build-10244857
- VMware vCenter Server 6.7.0 build-11727113
- VMware vCenter Server 6.7.0 build-14070654
- VMware vCenter Server 6.7.0 build-14792544
- VMware vCenter Server 6.7.0 build-15679289
- VMware vCenter Server 6.7.0 build-17137232
- VMware vCenter Server 6.7.0 build-17137327
- VMware vCenter Server 6.7.0 build-18010560
- VMware vCenter Server 6.7.0 build-18010599
- VMware vCenter Server 6.7.0 build-18485185
- VMware vCenter Server 6.7.0 build-18831049
- VMware vCenter Server 6.7.0 build-19299595
- VMware vCenter Server 6.7.0 build-19832280
- VMware vCenter Server 6.7.0 build-20504301
- VMware vCenter Server 6.7.0 build-20504362
- VMware vCenter Server 6.7.0 build-22509751
- VMware vCenter Server 6.7.0 build-24323669
- VMware vCenter Server 6.7.0 build-8170161
- VMware vCenter Server 7.0.2 build-17958471
- VMware vCenter Server 7.0.2 build-18356314
- VMware vCenter Server 7.0.2 build-18455184
- VMware vCenter Server 7.0.2 build-22781136
- VMware vCenter Server 7.0.3 build-18778458
- VMware vCenter Server 7.0.3 build-19234570
- VMware vCenter Server 7.0.3 build-19480866
- VMware vCenter Server 7.0.3 build-19717403
- VMware vCenter Server 7.0.3 build-20150588
- VMware vCenter Server 7.0.3 build-20395099
- VMware vCenter Server 7.0.3 build-20845200
- VMware vCenter Server 7.0.3 build-20990077
- VMware vCenter Server 7.0.3 build-21290409

- VMware vCenter Server 7.0.3 build-21477706
- VMware vCenter Server 7.0.3 build-21784236
- VMware vCenter Server 7.0.3 build-21958406
- VMware vCenter Server 7.0.3 build-22357613
- VMware vCenter Server 7.0.3 build-22837322
- VMware vCenter Server 7.0.3 build-23085514
- VMware vCenter Server 7.0.3 build-23788036
- VMware vCenter Server 7.0.3 build-24026615
- VMware vCenter Server 7.0.3 build-24201990
- VMware vCenter Server 7.0.3 build-24322018
- VMware vCenter Server 8.0.0 build-20519528
- VMware vCenter Server 8.0.0 build-20920323
- VMware vCenter Server 8.0.0 build-21216066
- VMware vCenter Server 8.0.0 build-21457384
- VMware vCenter Server 8.0.1 build-21560480
- VMware vCenter Server 8.0.1 build-21815093
- VMware vCenter Server 8.0.1 build-21860503
- VMware vCenter Server 8.0.1 build-22088981
- VMware vCenter Server 8.0.1 build-22368047
- VMware vCenter Server 8.0.1 build-24005165
- VMware vCenter Server 8.0.2 build-22385739
- VMware vCenter Server 8.0.2 build-22617221
- VMware vCenter Server 8.0.2 build-23319993
- VMware vCenter Server 8.0.2 build-23504390
- VMware vCenter Server 8.0.2 build-23929136
- VMware vCenter Server 8.0.2 build-24321653
- VMware vCenter Server 8.0.3 build-24022515
- VMware vCenter Server 8.0.3 build-24091160
- VMware vCenter Server 8.0.3 build-24262322
- VMware vCenter Server 8.0.3 build-24305161
- VMware vCenter Server 8.0.3 build-24322831

Prodotti supportati da questo raccoglitore dati:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
fondazione					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		Nome del nodo	Implementato	Servizi Web	
		OID	Implementato	Servizi Web	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**
		Tipo	Spacco	Servizi Web	
	Informazioni	Descrizione dell'API	Implementato	Servizi Web	
		Nome API	Implementato	Servizi Web	
		Versione API	Implementato	Servizi Web	
		Nome API client	Implementato	Servizi Web	
		Versione API client	Implementato	Servizi Web	
		Nome dell'origine dati	Implementato	Servizi Web	Informazioni
		Data	Implementato	Servizi Web	
		ID dell'originatore	Implementato	Servizi Web	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive
prestazione					
1410					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Informazioni aggiuntive

		velocità effettiva del disco				
		Lettura della	Implementato	Servizi Web		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Informazioni aggiuntive**	
		Portata totale	Implementato	Servizi Web	Throughput IP totale	
		ipThroughput.write	Implementato	Servizi Web		
		Utilizzo totale della memoria	Implementato	Servizi Web		
		swapRate.inRate	Implementato	Servizi Web		
		Tasso di swap	Implementato	Servizi Web		
		Tasso di swap totale	Implementato	Servizi Web		
		Pianifica il tempo di attesa	Implementato	Servizi Web	Tempo di attesa per la programmazione in percentuale	

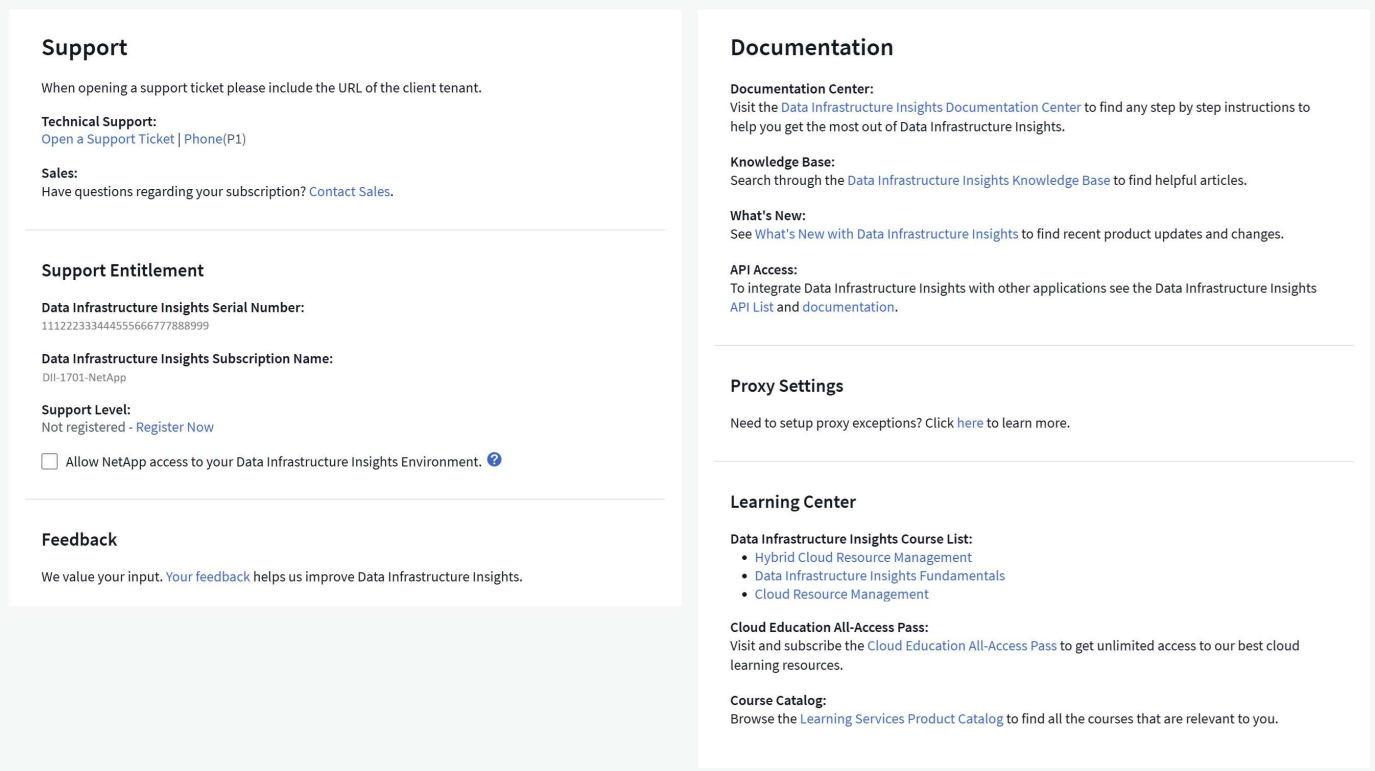
API di gestione utilizzate da questo raccoglitore dati:

API	Protocollo utilizzato	Protocollo di livello di trasporto utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di "sola lettura"	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST VMware	Servizi Web	HTTP/HTTPS	80/443		VERO	VERO	VERO	VERO

Riferimenti e supporto

Richiesta di supporto

È possibile accedere alle opzioni di supporto disponibili in Data Infrastructure Insights selezionando **Guida > Supporto**.



Attivazione del diritto al supporto

Data Infrastructure Insights offre supporto self-service e via e-mail durante l'esecuzione in modalità di prova. Una volta sottoscritto il servizio, si consiglia vivamente di attivare il diritto al supporto. L'attivazione del diritto di supporto consente di accedere al supporto tecnico tramite il sistema di ticketing web e telefono. La modalità di supporto predefinita è self-service fino al completamento della registrazione. Vederedettagli sotto.

Durante il processo di sottoscrizione iniziale, l'istanza di Data Infrastructure Insights genererà un numero di serie NetApp di 20 cifre che inizia con "950". Questo numero di serie NetApp rappresenta l'abbonamento a Data Infrastructure Insights associato al tuo account. Per attivare il diritto al supporto è necessario registrare il numero di serie NetApp . Offriamo due opzioni per la registrazione del supporto:

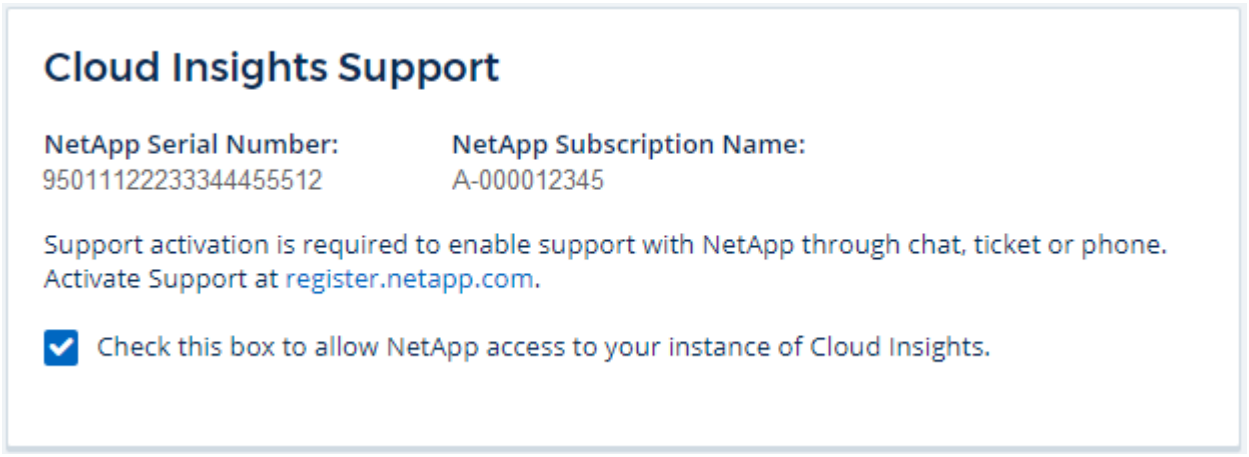
1. Utente con account SSO NetApp Support Site (NSS) preesistente (ad esempio, attuale cliente NetApp)
2. Nuovo cliente NetApp senza account SSO NetApp Support Site (NSS) preesistente

Opzione 1: Passaggi per un utente con un account SSO NetApp Support Site (NSS) preesistente

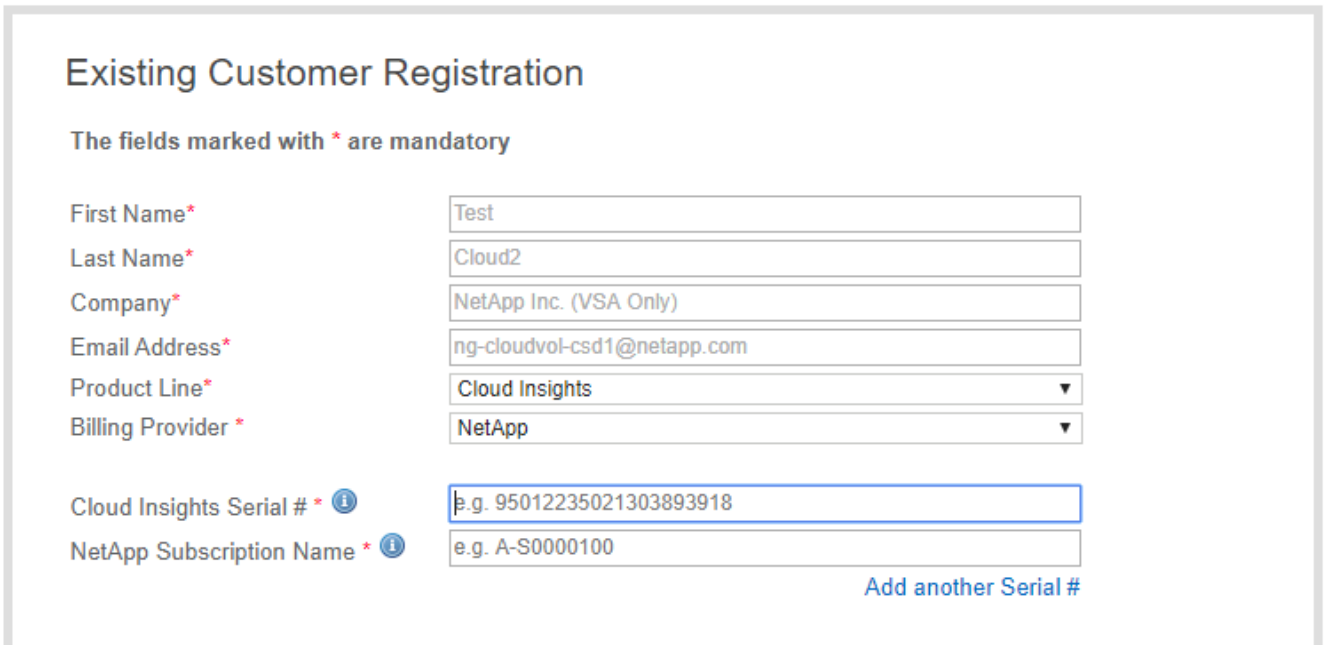
Passi

1. Vai al sito web di registrazione NetApp https://register.netapp.com
2. Seleziona "Sono già registrato come cliente NetApp " e scegli *Data Infrastructure Insights* come linea di prodotti. Seleziona il tuo fornitore di fatturazione (NetApp o AWS) e fornisci il tuo numero di serie e il nome

dell'abbonamento NetApp o l'ID cliente AWS facendo riferimento al menu **Aiuto › Supporto** nell'interfaccia utente Data Infrastructure Insights :



3. Compila il modulo di registrazione cliente esistente e clicca su **Invia**.

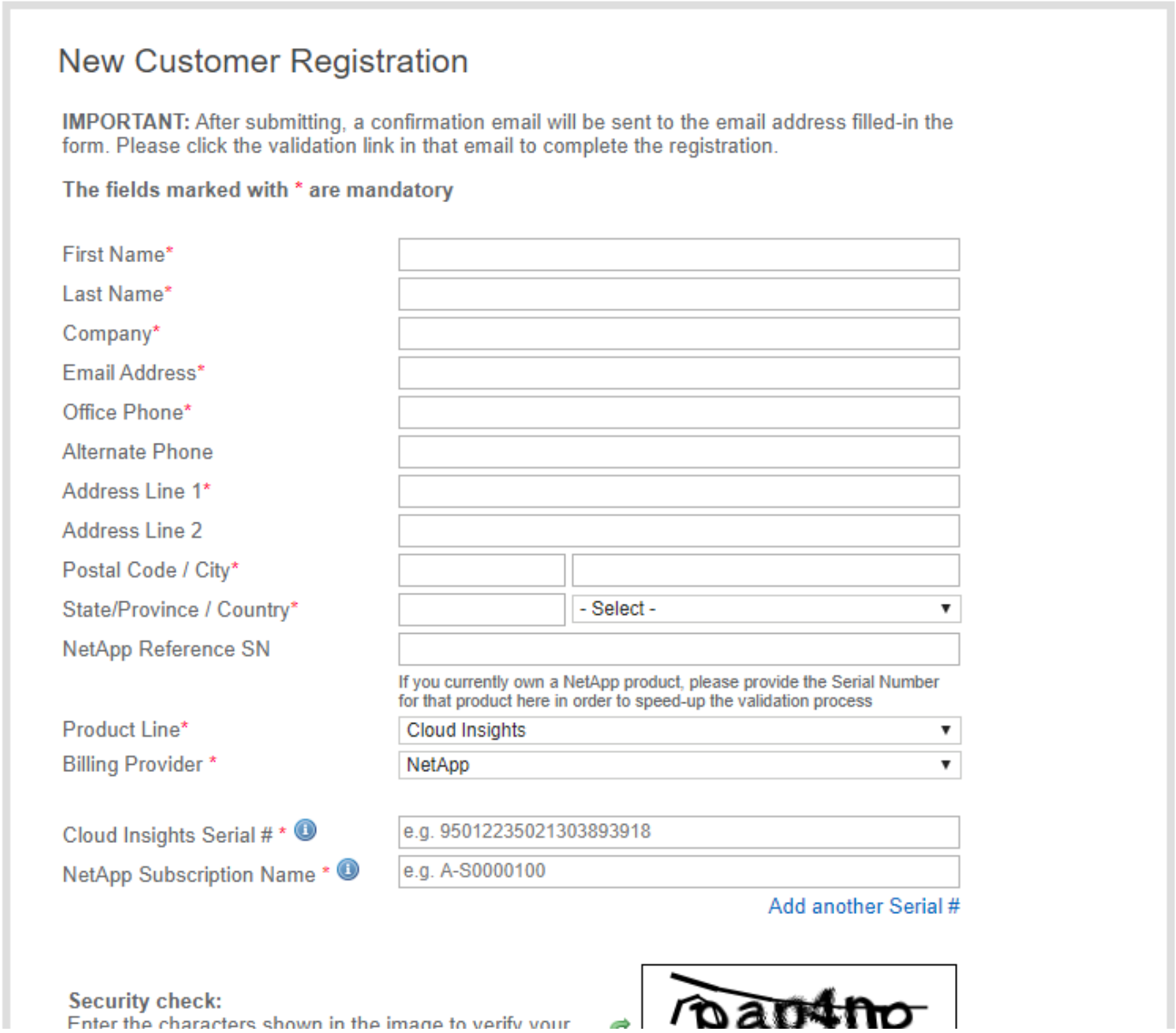


4. Se non si verificano errori, l'utente verrà indirizzato alla pagina "Registrazione inviata con successo". L'indirizzo email associato al nome utente NSS SSO utilizzato per la registrazione riceverà entro un paio di minuti un'email in cui si afferma che "il tuo prodotto è ora idoneo al supporto".
5. Questa è una registrazione una tantum per il numero di serie di Data Infrastructure Insights NetApp .

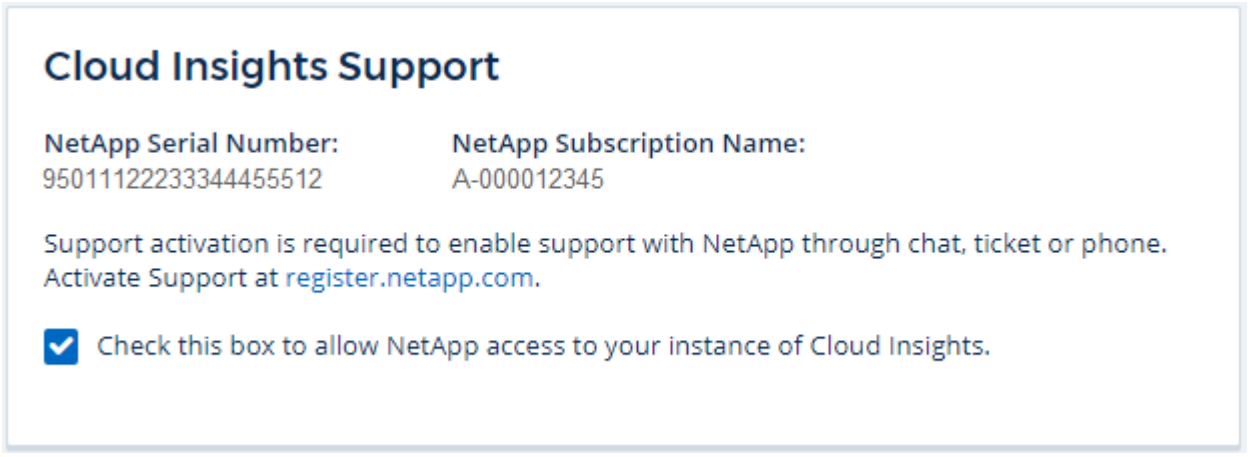
Opzione 2: Passaggi per un nuovo cliente NetApp senza un account SSO NetApp Support Site (NSS) preesistente

Passi

1. Vai al sito web di registrazione NetApp https://register.netapp.com
2. Seleziona "Non sono un cliente NetApp registrato" e compila le informazioni richieste nel modulo di esempio qui sotto:



1. Selezionare *Data Infrastructure Insights* come linea di prodotto. Seleziona il tuo fornitore di fatturazione (NetApp o AWS) e fornisci il tuo numero di serie e il nome dell'abbonamento NetApp o l'ID cliente AWS facendo riferimento al menu **Aiuto › Supporto** nell'interfaccia utente Data Infrastructure Insights :



2. Se non si verificano errori, l'utente verrà indirizzato alla pagina "Registrazione inviata con successo". L'indirizzo email associato al nome utente NSS SSO utilizzato per la registrazione riceverà entro poche ore un'email in cui si afferma che "il tuo prodotto è ora idoneo al supporto".
3. In qualità di nuovo cliente NetApp , dovrai anche creare un account utente NetApp Support Site (NSS) per le registrazioni future e per accedere al portale di supporto per il supporto tecnico e la gestione dei ticket web. Questo collegamento si trova a https://mysupport.netapp.com/eservice/public/now.do . Per velocizzare la procedura, puoi fornire il numero di serie Data Infrastructure Insights appena registrato.
4. Questa è una registrazione una tantum per il numero di serie di Data Infrastructure Insights NetApp .

Ottenere informazioni di supporto

NetApp fornisce supporto per Data Infrastructure Insights in vari modi. Sono disponibili ampie opzioni di auto-assistenza gratuite 24 ore su 24, 7 giorni su 7, come gli articoli della knowledge base (KB) o la community NetApp . Per gli utenti abbonati a Data Infrastructure Insights, il supporto tecnico è disponibile tramite telefono o ticketing web. Per i ticket Web e la gestione dei casi è necessario un account SSO NetApp Support Site (NSS).

Supporto self-service:

Queste opzioni di supporto sono disponibili in modalità di prova e sono disponibili gratuitamente 24 ore su 24, 7 giorni su 7:

- * https://kb.netapp.com/Cloud/ncds/nds/dii/dii_kbs [KnowledgeBase]*

  Facendo clic sui link in questa sezione si accede alla Knowledgebase NetApp , dove è possibile cercare articoli pertinenti, procedure guidate e altro ancora.

- *"Documentazione" *

  Cliccando sul link Documentazione si accede a questo centro di documentazione.

- *"Comunità" *

  Cliccando sul link della community verrai indirizzato alla community NetApp Data Infrastructure Insights , dove potrai entrare in contatto con colleghi ed esperti.

C'è anche un collegamento per fornire**"Feedback"** per aiutarci a migliorare Data Infrastructure Insights.

Supporto per l'abbonamento

Oltre alle opzioni di supporto autonomo sopra descritte, se disponi di un abbonamento a Data Infrastructure Insights o di supporto a pagamento per prodotti o servizi NetApp monitorati, puoi collaborare con un tecnico del supporto NetApp per risolvere il tuo problema.

Devi registrarti per poterattivare il supporto per i prodotti NetApp Cloud. Per registrarsi, andare sul sito di NetApp"Registrazione al supporto dei servizi dati cloud" .

Si consiglia vivamente di selezionare la casella per consentire a un tecnico del supporto NetApp di accedere al tenant di Data Infrastructure Insights durante la sessione di supporto. Ciò consentirà al tecnico di individuare il problema e di aiutarti a risolverlo rapidamente. Una volta risolto il problema o terminata la sessione di supporto, puoi deselezionare la casella.

Puoi richiedere supporto tramite uno dei seguenti metodi. Per utilizzare queste opzioni di supporto è

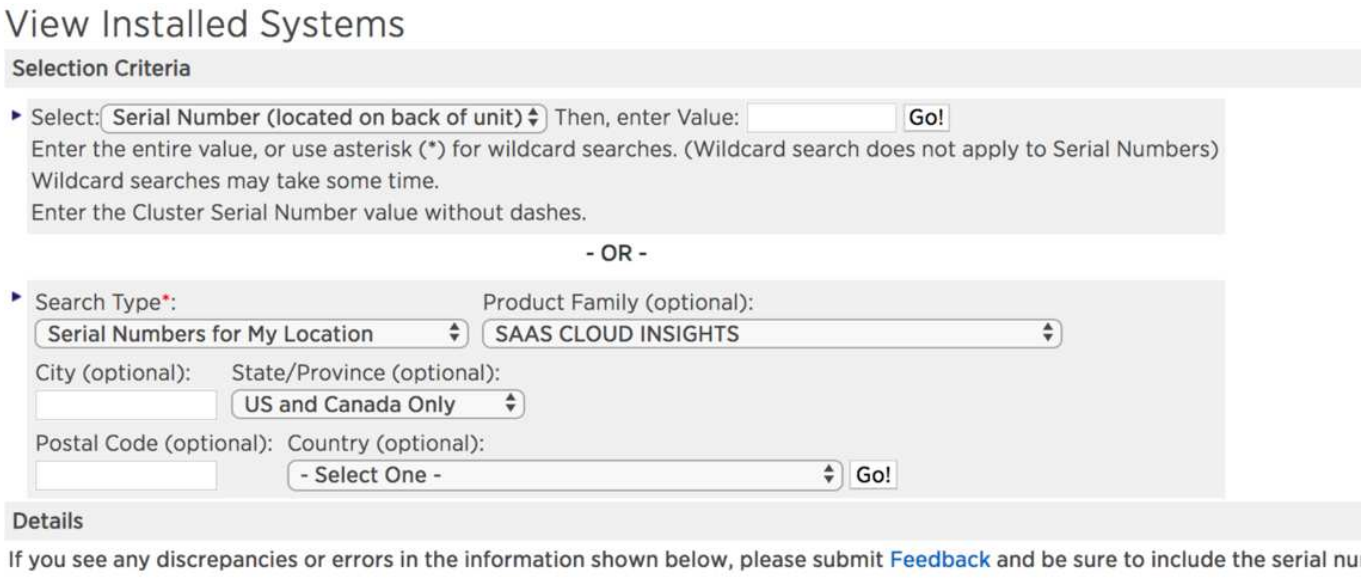
necessario disporre di un abbonamento attivo a Data Infrastructure Insights :

- **"Telefono"**
- **"Ticket di supporto"**

Puoi anche richiedere supporto alle vendite cliccando sul link **Contatta le vendite**.

Il numero di serie Data Infrastructure Insights è visibile all'interno del servizio dal menu **Aiuto > Supporto**. Se riscontri problemi nell'accesso al servizio e hai già registrato un numero di serie con NetApp , puoi anche visualizzare l'elenco dei numeri di serie di Data Infrastructure Insights dal sito di supporto NetApp come segue:

- Accedi a mysupport.netapp.com
- Dalla scheda del menu Prodotti > I miei prodotti, utilizza la famiglia di prodotti "SaaS Data Infrastructure Insights" per individuare tutti i numeri di serie registrati:



Matrice di supporto del collettore dati Data Infrastructure Insights

È possibile visualizzare o scaricare informazioni e dettagli sui Data Collector supportati in* Matrice di supporto del raccoglitore dati Data Infrastructure Insights *, ruolo= .

Centro di apprendimento

Indipendentemente dal tipo di abbonamento, **Aiuto > Supporto** contiene collegamenti a numerosi corsi offerti da NetApp University per aiutarti a sfruttare al meglio Data Infrastructure Insights. Date un'occhiata!

Riferimento al Data Collector - Infrastruttura

Riferimento specifico del fornitore

Gli argomenti in questa sezione forniscono informazioni di riferimento specifiche per ciascun fornitore. Nella maggior parte dei casi, la configurazione di un raccoglitore di dati è semplice. In alcuni casi, potrebbero essere necessarie informazioni o comandi aggiuntivi per configurare correttamente il raccoglitore dati.

Fare clic su un **fornitore** nel menu a sinistra per visualizzare le informazioni sui suoi raccoglitori di dati.

Configurazione del raccoglitore dati Amazon EC2

Data Infrastructure Insights utilizza il raccoglitore dati Amazon EC2 per acquisire dati di inventario e prestazioni dalle istanze EC2.

Requisiti

Per raccogliere dati dai dispositivi Amazon EC2, è necessario disporre delle seguenti informazioni:

- Devi avere uno dei seguenti requisiti:
  - Il **ruolo IAM** per il tuo account cloud Amazon EC2, se utilizzi l'autenticazione del ruolo IAM. Il ruolo IAM si applica solo se l'unità di acquisizione è installata su un'istanza AWS.
  - ID **Chiave di accesso IAM** e chiave di accesso segreta per il tuo account cloud Amazon EC2, se utilizzi l'autenticazione con chiave di accesso IAM.
- Devi avere il privilegio "organizzazione elenco"
- Porta 443 HTTPS
- Le istanze EC2 possono essere segnalate come macchine virtuali o (in modo meno naturale) come host. I volumi EBS possono essere segnalati sia come VirtualDisk utilizzato dalla VM, sia come DataStore che fornisce la capacità per VirtualDisk.

Le chiavi di accesso sono costituite da un ID chiave di accesso (ad esempio, AKIAIOSFODNN7EXAMPLE) e da una chiave di accesso segreta (ad esempio, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Le chiavi di accesso vengono utilizzate per firmare le richieste programmatiche inviate a EC2 se si utilizzano gli SDK di Amazon EC2, REST o le operazioni API di query. Queste chiavi sono fornite insieme al contratto Amazon.

Configurazione

Inserire i dati nei campi del raccoglitore dati secondo la tabella seguente:

Campo	Descrizione
Regione AWS	Scegli la regione AWS
Ruolo IAM	Da utilizzare solo se acquisito su un'AU in AWS. Vedi sotto per maggiori informazioni suRuolo IAM .
ID chiave di accesso AWS IAM	Inserisci l'ID della chiave di accesso AWS IAM. Obbligatorio se non si utilizza il ruolo IAM.
Chiave di accesso segreta AWS IAM	Inserisci la chiave di accesso segreta AWS IAM. Obbligatorio se non si utilizza il ruolo IAM.
Capisco che AWS mi fattura le richieste API	Seleziona questa opzione per verificare di aver compreso che AWS ti fattura le richieste API effettuate tramite polling di Data Infrastructure Insights .

Configurazione avanzata

Campo	Descrizione
Includi regioni extra	Specificare le regioni aggiuntive da includere nel sondaggio.
Ruolo multiaccount	Ruolo per l'accesso alle risorse in diversi account AWS.
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60
Scegli "Escludi" o "Includi" per applicare il filtro alle VM in base ai tag	Specificare se includere o escludere le VM tramite tag durante la raccolta dei dati. Se è selezionato "Includi", il campo Chiave tag non può essere vuoto.
Taggare chiavi e valori in base ai quali filtrare le VM	Fare clic su **+ Filtra tag** per scegliere quali VM (e dischi associati) includere/escludere filtrando le chiavi e i valori che corrispondono alle chiavi e ai valori dei tag sulla VM. La chiave tag è obbligatoria, il valore tag è facoltativo. Quando il valore del tag è vuoto, la VM viene filtrata finché corrisponde alla chiave del tag.
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 1800
Spazio dei nomi delle metriche dell'agente CloudWatch	Namespace in EC2/EBS da cui raccogliere i dati. Tieni presente che se i nomi delle metriche predefinite in questo spazio dei nomi vengono modificati, Data Infrastructure Insights potrebbe non essere in grado di raccogliere i dati rinominati. Si consiglia di lasciare i nomi predefiniti delle metriche.

Chiave di accesso IAM

Le chiavi di accesso sono credenziali a lungo termine per un utente IAM o per l'utente root dell'account AWS. Le chiavi di accesso vengono utilizzate per firmare richieste programmatiche all'AWS CLI o all'AWS API (direttamente o tramite l'AWS SDK).

Le chiavi di accesso sono composte da due parti: un ID della chiave di accesso e una chiave di accesso segreta. Quando si utilizza l'autenticazione *IAM Access Key* (anziché l'autenticazione *IAM Role*), è necessario utilizzare sia l'ID della chiave di accesso che la chiave di accesso segreta insieme per l'autenticazione delle richieste. Per maggiori informazioni, consulta la documentazione di Amazon su"Chiavi di accesso" .

Ruolo IAM

Quando si utilizza l'autenticazione *IAM Role* (anziché l'autenticazione IAM Access Key), è necessario assicurarsi che il ruolo creato o specificato disponga delle autorizzazioni appropriate necessarie per accedere alle risorse.

Ad esempio, se si crea un ruolo IAM denominato *InstanceEc2ReadOnly*, è necessario impostare il criterio per concedere a EC2 l'autorizzazione di accesso all'elenco di sola lettura per tutte le risorse EC2 per questo ruolo IAM. Inoltre, è necessario concedere l'accesso STS (Security Token Service) affinché questo ruolo possa assumere ruoli in più account.

Dopo aver creato un ruolo IAM, puoi allegarlo quando crei una nuova istanza EC2 o un'istanza EC2 esistente.

Dopo aver associato il ruolo IAM *InstanceEc2ReadOnly* a un'istanza EC2, sarà possibile recuperare le credenziali temporanee tramite i metadati dell'istanza in base al nome del ruolo IAM e utilizzarle per accedere alle risorse AWS da parte di qualsiasi applicazione in esecuzione su questa istanza EC2.

Per maggiori informazioni consulta la documentazione di Amazon su"Ruoli IAM" .

Nota: il ruolo IAM può essere utilizzato solo quando l'unità di acquisizione è in esecuzione in un'istanza AWS.

Mappatura dei tag Amazon alle annotazioni Data Infrastructure Insights

Il raccoglitore dati Amazon EC2 include un'opzione che consente di popolare le annotazioni di Data Infrastructure Insights con tag configurati su EC2. Le annotazioni devono essere denominate esattamente come i tag EC2. Data Infrastructure Insights popolerà sempre le annotazioni di tipo testo con lo stesso nome e farà un "miglior tentativo" per popolare le annotazioni di altri tipi (numero, valore booleano, ecc.). Se l'annotazione è di un tipo diverso e il raccoglitore dati non riesce a popolarla, potrebbe essere necessario rimuovere l'annotazione e ricrearla come tipo di testo.

Si noti che AWS distingue tra maiuscole e minuscole, mentre Data Infrastructure Insights non distingue tra maiuscole e minuscole. Pertanto, se si crea un'annotazione denominata "OWNER" in Data Infrastructure Insights e tag denominati "OWNER", "Owner" e "owner" in EC2, tutte le varianti EC2 di "owner" verranno mappate all'annotazione "OWNER" di Cloud Insight.

Includi regioni extra

Nella sezione **Configurazione avanzata** di AWS Data Collector, puoi impostare il campo **Includi regioni extra** per includere regioni aggiuntive, separate da virgola o punto e virgola. Per impostazione predefinita, questo campo è impostato su ***us-.****, che raccoglie dati in tutte le regioni AWS degli Stati Uniti. Per raccogliere dati su *tutte* le regioni, impostare questo campo su ***.****. Se il campo **Includi regioni extra** è vuoto, il raccoglitore dati raccoglierà i dati sulle risorse specificate nel campo **Regione AWS** come specificato nella sezione **Configurazione**.

Raccolta da account figlio AWS

Data Infrastructure Insights supporta la raccolta di account figlio per AWS all'interno di un singolo raccoglitore dati AWS. La configurazione per questa raccolta viene eseguita nell'ambiente AWS:

- È necessario configurare ogni account figlio in modo che disponga di un ruolo AWS che consenta all'ID dell'account principale di accedere ai dettagli EC2 dall'account figlio.
- Ogni account figlio deve avere il nome del ruolo configurato come la stessa stringa.
- Inserisci questa stringa del nome del ruolo nella sezione **Configurazione avanzata** di Data Infrastructure Insights AWS Data Collector, nel campo **Ruolo tra account**.
- L'account in cui è installato il collector deve disporre dei privilegi di *amministratore di accesso delegato*. Vedi il"Documentazione AWS" per maggiori informazioni.

Best Practice: si consiglia vivamente di assegnare la policy predefinita AWS *AmazonEC2ReadOnlyAccess* all'account principale EC2. Inoltre, all'utente configurato nell'origine dati deve essere assegnata almeno la policy predefinita *AWSOrganizationsReadOnlyAccess* per poter interrogare AWS.

Per informazioni sulla configurazione dell'ambiente per consentire a Data Infrastructure Insights di raccogliere dati dagli account figlio AWS, consultare quanto segue:

"Tutorial: delegare l'accesso tra account AWS utilizzando i ruoli IAM"

"Configurazione AWS: fornire l'accesso a un utente IAM in un altro account AWS di tua proprietà"

"Creazione di un ruolo per delegare le autorizzazioni a un utente IAM"

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Amazon FSx for NetApp ONTAP

Questo raccoglitore di dati acquisisce dati di inventario e prestazioni da Amazon FSx for NetApp ONTAP. Questo strumento di raccolta dati verrà reso disponibile in modo incrementale in tutte le regioni del servizio Data Infrastructure Insights . Contatta il tuo addetto alle vendite se non vedi l'icona per questo raccoglitore nel tuo ambiente Data Infrastructure Insights .

> Questo raccoglitore di Data Infrastructure Insights richiede un utente ONTAP con un ruolo *Filesystem-Scoped*. Si prega di rivedere l'AWS"Ruoli e regole" documentazione per le opzioni disponibili. Al momento AWS supporta solo un tipo di ruolo utente con ambito filesystem, ovvero *fsxadmin*. Questo è il ruolo appropriato da utilizzare per il raccoglitore Data Infrastructure Insights . All'utente dovrebbero essere assegnate tutte e tre queste applicazioni: http, ontapi, ssh.

Terminologia

Data Infrastructure Insights acquisisce dati di inventario e prestazioni dal raccoglitore dati FSx- NetApp . Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per l'asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Grappolo	Magazzinaggio
LUN	Volume
Volume	Volume interno

Terminologia FSx- NetApp

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle pagine di destinazione delle risorse di storage FSx- NetApp . Molti di questi termini si applicano anche ad altri raccoglitori di dati.

Magazzinaggio

- Modello: elenco delimitato da virgole dei nomi di modelli univoci e discreti all'interno di questo cluster.
- Fornitore – AWS
- Numero di serie: il numero di serie dell'array.
- IP: in genere saranno gli IP o i nomi host configurati nell'origine dati.
- Capacità grezza: somma in base 2 di tutto lo spazio di archiviazione SSD assegnato al file system FSx.
- Latenza: rappresentazione di ciò che sta sperimentando l'host sottoposto a carichi di lavoro, sia in lettura che in scrittura. Idealmente, Data Infrastructure Insights reperirebbe questo valore direttamente, ma spesso non è così. Invece dell'array che offre questa funzionalità, Data Infrastructure Insights esegue in genere un calcolo ponderato in base agli IOPS derivato dalle statistiche dei singoli volumi interni.

- Capacità di elaborazione: aggregata dai volumi interni. Gestione: può contenere un collegamento ipertestuale all'interfaccia di gestione del dispositivo. Creato a livello di programmazione dalla fonte dati Data Infrastructure Insights come parte della reportistica di inventario.

Pool di archiviazione

- Archiviazione: su quale array di archiviazione risiede questo pool. Obbligatorio.
- Tipo: un valore descrittivo da un elenco di possibilità enumerate. Nella maggior parte dei casi sarà "Aggregato" o "Gruppo RAID".
- Capacità: i valori qui indicati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata tra queste.
- IOPS: la somma degli IOPS di tutti i volumi allocati su questo pool di archiviazione.
- Throughput: la somma del throughput di tutti i volumi allocati su questo pool di archiviazione.

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questo raccoglitore dati:

- Devi avere accesso a un account con il ruolo "fsxadmin", con tre applicazioni assegnate: ssh, ontapi, http
- I dettagli dell'account includono nome utente e password.
- Requisiti della porta: 443

Configurazione

Campo	Descrizione
IP di gestione NetApp	Indirizzo IP o nome di dominio completo del cluster NetApp
Nome utente	Nome utente per il cluster NetApp
Password	Password per il cluster NetApp

Metriche avanzate

Questo raccoglitore di dati raccoglie le seguenti metriche avanzate dall'archiviazione FSx per NetApp ONTAP :

- politica
- nfsv3
- nfsv3:nodo
- nfsv4
- nfsv4_1
- nfsv4_1:nodo
- nfsv4:nodo
- gruppo_politiche
- qtree
- volume

- volume_del_carico_di_lavoro

Si noti che i comandi API e CLI di FSx recuperano alcuni valori di capacità che Data Infrastructure Insights ZAPI non raccoglie, pertanto alcuni valori di capacità (ad esempio quelli per i pool di archiviazione) potrebbero essere diversi in Data Infrastructure Insights rispetto a quelli presenti su FSx stesso.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Ricevi la risposta HTTP 401 o il codice di errore ZAPI 13003 e ZAPI restituisce "Privilegi insufficienti" o "non autorizzato per questo comando"	Controllare nome utente, password e privilegi/permessi dell'utente.
ZAPI restituisce "il ruolo del cluster non è cluster_mgmt LIF"	L'AU deve comunicare con l'IP di gestione del cluster. Controllare l'IP e, se necessario, cambiarlo con un IP diverso
Il comando ZAPI fallisce dopo il nuovo tentativo	L'AU ha problemi di comunicazione con il cluster. Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare a eseguire un comando dalla riga di comando della macchina AU.
AU non è riuscito a connettersi a ZAPI tramite HTTP	Verificare se la porta ZAPI accetta testo in chiaro. Se AU tenta di inviare testo in chiaro a un socket SSL, la comunicazione fallisce.
La comunicazione fallisce con SSLException	AU sta tentando di inviare SSL a una porta in chiaro su un filer. Verificare se la porta ZAPI accetta SSL oppure utilizzare una porta diversa.
Errori di connessione aggiuntivi: la risposta ZAPI ha il codice di errore 13001, "database non aperto". Il codice di errore ZAPI è 60 e la risposta contiene "API non completata in tempo". La risposta ZAPI contiene "initialize_session() ha restituito ambiente NULL". Il codice di errore ZAPI è 14007 e la risposta contiene "Nodo non funzionante".	Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare a eseguire un comando dalla riga di comando della macchina AU.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati di calcolo di Azure

Data Infrastructure Insights utilizza il raccoglitore dati di calcolo di Azure per acquisire dati di inventario e prestazioni dalle istanze di calcolo di Azure.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni.

- Requisito porta: 443 HTTPS

- URI di reindirizzamento Azure OAuth 2.0 (login.microsoftonline.com)
- IP REST di gestione di Azure (management.azure.com)
- IP di Azure Resource Manager (management.core.windows.net)
- ID applicazione Azure Service Principal (client) (ruolo di lettore richiesto)
- Chiave di autenticazione dell'entità servizio di Azure (password utente)
- È necessario configurare un account Azure per l'individuazione di Data Infrastructure Insights .

  Una volta configurato correttamente l'account e registrata l'applicazione in Azure, si avranno le credenziali necessarie per individuare l'istanza di Azure con Data Infrastructure Insights. Il seguente collegamento descrive come impostare l'account per la scoperta.https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal[]

Configurazione

Inserire i dati nei campi del raccoglitore dati secondo la tabella seguente:

Campo	Descrizione
ID applicazione Azure Service Principal (client) (ruolo di lettore richiesto)	ID di accesso ad Azure. Richiede l'accesso al ruolo di Lettore.
ID tenant di Azure	ID tenant Microsoft
Chiave di autenticazione dell'entità servizio di Azure	Chiave di autenticazione di accesso
Capisco che Microsoft mi fattura le richieste API	Seleziona questa casella per verificare di aver compreso che Microsoft ti addebita le richieste API effettuate tramite polling di Insight.

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60
Scegli "Escludi" o "Includi" per applicare il filtro alle VM in base ai tag	Specificare se includere o escludere le VM tramite tag durante la raccolta dei dati. Se è selezionato "Includi", il campo Chiave tag non può essere vuoto.
Taggare chiavi e valori in base ai quali filtrare le VM	Fare clic su **+ Filtra tag** per scegliere quali VM (e dischi associati) includere/escludere filtrando le chiavi e i valori che corrispondono alle chiavi e ai valori dei tag sulla VM. La chiave tag è obbligatoria, il valore tag è facoltativo. Quando il valore del tag è vuoto, la VM viene filtrata finché corrisponde alla chiave del tag.
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 300

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Broadcom

Raccoglitore dati Brocade Network Advisor

Data Infrastructure Insights utilizza il raccoglitore dati Brocade Network Advisor per acquisire dati di inventario e prestazioni dagli switch Brocade .

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Brocade Network Advisor. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Interruttore	Interruttore
Porta	Porta
Tessuto virtuale, tessuto fisico	Tessuto
Interruttore logico	Interruttore logico

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessari i seguenti elementi:

- L'unità di acquisizione Data Infrastructure Insights avvierà le connessioni alla porta TCP 443 sul server BNA. Il server BNA deve eseguire la versione 14.2.1 o successiva.
- Indirizzo IP del server Brocade Network Advisor
- Nome utente e password per un account amministratore
- Requisito porta: HTTP/HTTPS 443

Configurazione

Campo	Descrizione
IP del server Brocade Network Advisor	Indirizzo IP del server Network Advisor
Nome utente	Nome utente per lo switch
Nome utente	Nome utente amministratore
Password	Password dell'amministratore

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS (porta predefinita 443) o HTTP (porta predefinita 80)

Campo	Descrizione
Sostituisci porta di connessione	Se vuoto, utilizzare la porta predefinita nel campo Tipo di connessione, altrimenti immettere la porta di connessione da utilizzare
Password	Password per lo switch
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 40
Gateway di accesso ai report	Selezionare per includere i dispositivi in modalità Access Gateway
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 1800

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Ricevi un messaggio che indica che più di un nodo è connesso alla porta Access Gateway oppure che il raccoglitore dati non riesce a rilevare il dispositivo Access Gateway.	Verificare che il dispositivo NPV funzioni correttamente e che tutti i WWN collegati siano previsti. Non acquistare direttamente il dispositivo NPV. Invece, l'acquisizione dello switch core fabric raccoglierà i dati del dispositivo NPV.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Brocade FC Switch

Data Infrastructure Insights utilizza la fonte dati Brocade FC Switch (SSH) per scoprire l'inventario dei dispositivi switch Brocade o rinominati che eseguono il firmware Factored Operating System (FOS) 4.2 e versioni successive. Sono supportati i dispositivi sia in modalità switch FC che Access Gateway.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Brocade FC Switch. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Interruttore	Interruttore
Porta	Porta
Tessuto virtuale, tessuto fisico	Tessuto
Zona	Zona

Termine del fornitore/modello	Termine Data Infrastructure Insights
Interruttore logico	Interruttore logico
Volume virtuale	Volume
Zona LSAN	Zona IVR

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- L'unità di acquisizione (AU) Data Infrastructure Insights avvierà le connessioni alla porta TCP 22 sugli switch Brocade per raccogliere i dati di inventario. L'AU avvierà anche connessioni alla porta UDP 161 per la raccolta dei dati sulle prestazioni.
- Deve essere presente connettività IP per tutti gli switch nel fabric. Se selezioni la casella di controllo Scopri tutti gli switch nel fabric, Data Infrastructure Insights identifica tutti gli switch nel fabric; tuttavia, necessita della connettività IP a questi switch aggiuntivi per rilevarli.
- È necessario lo stesso account a livello globale su tutti gli switch del fabric. Per confermare l'accesso è possibile utilizzare PuTTY (emulatore di terminale open source).
- Le porte 161 e 162 devono essere aperte a tutti gli switch nel fabric per il polling delle prestazioni SNMP.
- Stringa di comunità SNMP di sola lettura

Configurazione

Campo	Descrizione
Cambia IP	Indirizzo IP o nome di dominio completo del server EFC
Nome utente	Nome utente per lo switch
Password	Password per lo switch
SNMP	Versione SNMP
Stringa della comunità SNMP	Stringa di comunità SNMP di sola lettura utilizzata per accedere allo switch
Nome utente SNMP	Nome utente SNMP
Password SNMP	password SNMP

Configurazione avanzata

Campo	Descrizione
Nome del tessuto	Nome del tessuto che deve essere segnalato dal raccoglitore dati. Lasciare vuoto per segnalare il nome del tessuto come WWN.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 15.

Campo	Descrizione
Dispositivi esclusi	Elenco separato da virgole degli ID dispositivo da escludere dal polling
Domini amministrativi attivi	Selezionare se si utilizzano domini amministrativi
Recupera i dati MPR	Selezionare per acquisire i dati di routing dal router multiprotocollo.
Abilita Trapping	Selezionare per abilitare l'acquisizione alla ricezione di una trap SNMP dal dispositivo. Se si seleziona Abilita trapping, è necessario attivare anche SNMP.
Tempo minimo tra le trappole (sec)	Tempo minimo tra i tentativi di acquisizione attivati dalle trappole. Il valore predefinito è 10.
Scopri tutti gli interruttori nel tessuto	Seleziona per scoprire tutti gli switch nel fabric
Scegli di preferire HBA rispetto agli alias di zona	Scegli se favorire gli alias HBA o di zona
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300.
Protocollo di autenticazione SNMP	Protocollo di autenticazione SNMP (solo SNMP v3)
Password di privacy SNMP	Password di privacy SNMP (solo SNMP v3)
Tentativi SNMP	Numero di tentativi di ripetizione SNMP

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
L'acquisizione dell'inventario della sorgente dati Brocade non riesce con l'errore: <data> <ora> ERRORE [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Errore 2 su 2: <nome sorgente dati> [Errore interno] - Impossibile generare il modello per il dispositivo <IP>. Errore durante il rilevamento del prompt ([Nome dispositivo <nome>]: Impossibile generare il modello per il dispositivo <IP>. Errore durante il rilevamento del prompt)	Il problema potrebbe verificarsi quando lo switch Brocade impiega troppo tempo per rispondere a un prompt, superando il timeout predefinito di 5 secondi. Nelle impostazioni di Configurazione avanzata del raccoglitore dati in Data Infrastructure Insights, prova ad aumentare il valore di *Timeout di attesa banner SSH (sec)* a un valore più alto.
Errore: "Data Infrastructure Insights ha ricevuto un ruolo chassis non valido"	Verificare che all'utente configurato in questa origine dati sia stata concessa l'autorizzazione al ruolo chassis.

Problema:	Prova questo:
Errore: "Indirizzo IP dello chassis non corrispondente"	Di norma, DII NON supporta la traduzione degli indirizzi di rete o la traduzione degli indirizzi di porta tra l'unità di acquisizione e i dispositivi. DII potrebbe rilevare che il nome host/indirizzo IP nella configurazione del collettore NON corrisponde a nessuno degli indirizzi che il dispositivo ritiene di avere.
Ricevi un messaggio che indica che più di un nodo è connesso alla porta Access Gateway	Verificare che il dispositivo NPV funzioni correttamente e che tutti i WWN collegati siano previsti. Non acquistare direttamente il dispositivo NPV. Invece, l'acquisizione dello switch core fabric raccoglierà i dati del dispositivo NPV.
Errore: ….Numero massimo di sessioni remote per l'accesso…	FOS ha limiti diversi per il numero di sessioni SSH contemporanee supportate per ruolo utente. La sessione SSH di DII su questo dispositivo viene rifiutata all'accesso perché viola tali limiti. Questo può essere un segnale che dei collezionisti duplicatori stanno scoprendo lo stesso bene, cosa che dovrebbe essere evitata

Prestazione

Problema:	Prova questo:
La raccolta delle prestazioni non riesce con "Timeout durante l'invio della richiesta SNMP".	A seconda delle variabili di query e della configurazione dello switch, alcune query potrebbero superare il timeout predefinito. "Saperne di più" .
La raccolta delle prestazioni non riesce con …Righe duplicate trovate nella tabella SNMP…	DII ha rilevato risposte SNMP errate. Probabilmente stai utilizzando FOS 8.2.3e. Aggiorna alla versione 8.2.3e2 o successiva.
La raccolta delle prestazioni non riesce con …Nome utente sconosciuto…	Hai configurato il tuo raccoglitore DII con un valore "Nome utente SNMP" che non è inserito in uno degli slot utente SNMPv3. La semplice creazione di un utente su Brocade FOS NON lo abilita necessariamente come utente SNMPv3: è necessario inserirlo in uno degli slot utente v3.
Le raccolte di prestazioni non riescono con …Livello di sicurezza non supportato…	Hai configurato il tuo raccoglitore DII per utilizzare SNMPv3, ma con impostazioni di crittografia (ovvero privacy) e/o di autorizzazione non abilitate sul dispositivo in questione.
La raccolta delle prestazioni non riesce con …La password di privacy vuota è consentita solo per il protocollo di privacy NESSUNO	Hai configurato il tuo raccoglitore DII per utilizzare SNMPv3, con un protocollo di crittografia noto anche come protocollo di privacy (AES, ecc.), ma hai un valore "SNMP Privacy Password" vuoto, quindi DII non può negoziare flussi di dati SNMPv3 crittografati con questo dispositivo

Problema:	Prova questo:
La raccolta delle prestazioni fallisce con …..VF:nn, errore: nessun accesso…	Hai configurato il tuo raccoglitore DII per utilizzare SNMPv3 su un dispositivo con più Virtual Fabric abilitati, ma l'utente SNMPv3 NON ha diritti per VF NN. DII non supporta la scoperta parziale di una risorsa fisica: dovresti sempre concedere a DII l'accesso a tutti i 128 VF possibili in modo proattivo, poiché DII tenterà sempre di recuperare i dati sulle prestazioni per qualsiasi VF esistente su un dato dispositivo fisico.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Brocade FOS REST Data Collector

Data Infrastructure Insights utilizza il raccoglitore REST Brocade FOS per scoprire l'inventario e le prestazioni dei dispositivi switch Brocade che eseguono il firmware FabricOS (FOS) 8.2 e versioni successive. Si prega di notare che le prime versioni 8.2 FOS potrebbero presentare bug nell'API REST; si consiglia vivamente di eseguire l'ultima versione FOS supportata dalla piattaforma.

Nota: il livello "utente" predefinito di FOS non è sufficientemente potente per consentire a Data Infrastructure Insights di visualizzare tutti gli aspetti logici di un dispositivo. È necessario un account utente con il "Ruolo chassis" abilitato, nonché autorizzazioni su tutti i Virtual Fabric configurati su uno switch.

Ecco un esempio di come creare un account utente con "privilegi minimi" per l'utilizzo di Data Infrastructure Insights in una sessione SSH su un dispositivo FOS:

userConfig --add NetAppCIUser -r utente -l 1-128 -c utente -p Qwerty!

Verrà creato un utente "NetAppCIUser" con password "Qwerty!". Questo utente ha il ruolo "utente" (-r) in tutti i 128 possibili fabric virtuali (-l). Questo utente ha inoltre il ruolo "Chassis" richiesto (-c) con accesso a livello utente assegnato.

Per impostazione predefinita, questo collector tenterà di rilevare tutti i dispositivi FOS che fanno parte di tutti i fabric di cui fa parte lo switch.

Nota: l'utente di sola lettura predefinito di FOS, "user", NON dispone di autorizzazioni di visualizzazione su tutti i Virtual Fabric, né di autorizzazioni di "ruolo chassis". Ciò significa che le probabilità di successo saranno basse utilizzando "user" con Data Infrastructure Insights, che deve comprendere sia la configurazione fisica che quella logica del dispositivo FOS.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Brocade FOS REST. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Interruttore	Interruttore
Porta	Porta
Tessuto virtuale, tessuto fisico	Tessuto
Zona	Zona
Interruttore logico	Interruttore logico
Zona LSAN	Zona IVR

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Deve esserci connettività TCP su tutti gli switch nel fabric. Questo tipo di raccoglitore di dati proverà senza problemi sia HTTP che HTTPS per ogni dispositivo nel fabric. Se selezioni la casella di controllo *Scopri tutti gli switch nel fabric*, Data Infrastructure Insights identifica tutti gli switch nel fabric; tuttavia, necessita della connettività TCP a questi switch aggiuntivi per rilevarli.
- È necessario lo stesso account a livello globale su tutti gli switch del fabric. È possibile utilizzare l'interfaccia Web del dispositivo per confermare l'accesso.

Configurazione

Campo	Descrizione
Cambia IP	Indirizzo IP o nome di dominio completo dello switch FOS
Nome utente	Nome utente per lo switch
Password	Password per lo switch

Configurazione avanzata

Campo	Descrizione
Dispositivi esclusi	Elenco separato da virgole degli indirizzi IPv4 dei dispositivi da escludere dal polling.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60.
Scopri tutti gli interruttori nel tessuto	Seleziona per scoprire tutti gli switch nel fabric.
Scegli di preferire HBA rispetto agli alias di zona	Scegliere se privilegiare HBA o alias di zona.
Tipo di connessione	HTTP o HTTPS.
Si noti che questa impostazione modifica solo il protocollo che CI tenta di utilizzare per primo per dispositivo: CI tenterà automaticamente il protocollo opposto se il valore predefinito fallisce.	Sostituisci porta TCP

Campo	Descrizione
Specificare una porta se non si utilizza quella predefinita.	Intervallo di sondaggio sulle prestazioni (sec)

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
La funzione Test mi avvisa che un protocollo non è accessibile	Un dato dispositivo Brocade FOS 8.2+ vorrà comunicare solo tramite HTTP o HTTPS: se uno switch ha un certificato digitale installato, genererà errori HTTP se si tenta di comunicare con esso tramite HTTP non crittografato anziché HTTPS. La funzione di test tenta la comunicazione sia con HTTP che con HTTPS: se il test indica che un protocollo funziona, è possibile salvare in sicurezza il collettore e non preoccuparsi che l'altro protocollo non abbia avuto successo: il collettore tenterà entrambi i protocolli durante la raccolta e fallirà solo se nessuno dei due funziona.
Errore: l'inventario fallisce con 401 Non autorizzato… Chiave di sessione non valida…	Si tratta di un bug specifico presente in alcune delle prime versioni 8.2 FOS, come la 8.2.1c, che NON supportano correttamente l'autenticazione di base HTTP. Aggiorna a una versione successiva 8.2 o 9.*
Errore: "Data Infrastructure Insights ha ricevuto un ruolo chassis non valido"	Verificare che all'utente configurato in questa origine dati sia stata concessa l'autorizzazione al ruolo chassis.
Errore: "Indirizzo IP dello chassis non corrispondente"	Modificare la configurazione dell'origine dati per utilizzare l'indirizzo IP dello chassis.
L'inventario fallisce con un errore 403 Forbidden	Potrebbe trattarsi semplicemente di credenziali errate oppure potrebbe indicare che si sta tentando di utilizzare un ruolo non sufficientemente potente. Ricordare che gli utenti di livello "utente" NON hanno il diritto "Ruolo chassis" richiesto né l'accesso alla visualizzazione di Virtual Fabric non predefiniti.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Cisco MDS Fabric Switch

Data Infrastructure Insights utilizza il raccoglitore dati Cisco MDS Fabric Switches per scoprire l'inventario per Cisco MDS Fabric Switches e una varietà di switch Cisco Nexus FCoE su cui è abilitato il servizio FC.

Inoltre, con questo raccoglitore di dati è possibile scoprire molti modelli di dispositivi Cisco che funzionano in

modalità NPV.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Cisco FC Switch. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Interruttore	Interruttore
Porta	Porta
VSAN	Tessuto
Zona	Zona
Interruttore logico	Interruttore logico
Voce del server dei nomi	Voce del server dei nomi
Zona di routing inter-VSAN (IVR)	Zona IVR

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Un indirizzo IP di uno switch nel fabric o di singoli switch
- Scoperta dello chassis, per abilitare la scoperta del fabric
- Se si utilizza SNMP V2, stringa di comunità di sola lettura
- La porta 161 viene utilizzata per accedere al dispositivo

Configurazione

Campo	Descrizione
IP dello switch Cisco	Indirizzo IP o nome di dominio completo dello switch
Versione SNMP	Selezionare V1, V2 o V3. Per l'acquisizione delle prestazioni è richiesta la versione V2 o successiva.
Stringa della comunità SNMP	Stringa di comunità SNMP di sola lettura utilizzata per accedere allo switch (non applicabile per SNMP v3)
Nome utente	Nome utente per lo switch (solo SNMP v3)
Password	Password utilizzata per lo switch (solo SNMPv3)

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi dell'inventario (predefinito 40 minuti)

Campo	Descrizione
Protocollo di autenticazione SNMP	Protocollo di autenticazione SNMP (solo SNMPv3)
Protocollo di privacy SNMP	Protocollo di privacy SNMP (solo SNMPv3)
Password di privacy SNMP	Password di privacy SNMP
Tentativi SNMP	Numero di tentativi di ripetizione SNMP
Timeout SNMP (ms)	Timeout SNMP (predefinito 5000 ms)
Abilita Trapping	Selezionare per abilitare il trapping. Se si abilita il trapping, è necessario attivare anche le notifiche SNMP.
Tempo minimo tra le trappole (sec)	Tempo minimo tra i tentativi di acquisizione attivati dalle trappole (predefinito 10 secondi)
Scopri tutti gli interruttori in tessuto	Seleziona per scoprire tutti gli switch nel fabric
Dispositivi esclusi	Elenco separato da virgole degli IP dei dispositivi da escludere dal polling
Dispositivi inclusi	Elenco separato da virgole degli IP dei dispositivi da includere nel polling
Controlla il tipo di dispositivo	Selezionare per accettare solo i dispositivi che si pubblicizzano esplicitamente come dispositivi Cisco
Primo tipo di alias	Fornire una prima preferenza per la risoluzione dell'alias. Scegliere tra le seguenti: **Device Alais** Si tratta di un nome di facile utilizzo per una porta WWN (pWWN) che può essere utilizzato in tutti i comandi di configurazione, a seconda delle necessità. Tutti gli switch della famiglia Cisco MDS 9000 supportano i servizi Distributed Device Alias (alias dei dispositivi). **Nessuno** Non segnalare alcun alias. **Descrizione della porta** Una descrizione che aiuta a identificare la porta in un elenco di porte. **Alias di zona (tutti)** Un nome di facile utilizzo per una porta che può essere utilizzata solo per la configurazione attiva. Questa è l'impostazione predefinita.
Secondo tipo di alias	Fornire una seconda preferenza per la risoluzione dell'alias
Terzo tipo di alias	Fornire una terza preferenza per la risoluzione dell'alias
Abilita il supporto della modalità proxy SANTap	Seleziona se il tuo switch Cisco utilizza SANTap in modalità proxy. Se utilizzi EMC RecoverPoint, probabilmente stai utilizzando SANTap.
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni (predefinito 300 secondi)

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: Impossibile rilevare lo chassis. Non sono stati rilevati switch.	• Eseguire il ping del dispositivo con l'IP configurato • Accedere al dispositivo utilizzando l'interfaccia grafica utente Cisco Device Manager • Accedere al dispositivo utilizzando la CLI • Provare a eseguire SNMP walk
Errore: il dispositivo non è uno switch Cisco MDS	• Assicurarsi che l'IP della sorgente dati configurato per il dispositivo sia corretto • Accedere al dispositivo utilizzando l'interfaccia utente grafica Cisco Device Manager • Accedere al dispositivo utilizzando la CLI
Errore: Data Infrastructure Insights non è in grado di ottenere il WWN dello switch.	Potrebbe non trattarsi di uno switch FC o FCoE e, in quanto tale, potrebbe non essere supportato. Assicurarsi che l'IP/FQDN configurato nell'origine dati sia effettivamente uno switch FC/FCoE.
Errore: sono stati trovati più nodi connessi alla porta dello switch NPV	Disabilitare l'acquisizione diretta dello switch NPV
Errore: impossibile connettersi allo switch	• Assicurarsi che il dispositivo sia ATTIVO • Controllare l'indirizzo IP e la porta di ascolto • Eseguire il ping del dispositivo • Accedere al dispositivo utilizzando l'interfaccia utente grafica Cisco Device Manager • Accedere al dispositivo utilizzando la CLI • Eseguire SNMP walk

Prestazione

Problema:	Prova questo:
Errore: acquisizione delle prestazioni non supportata da SNMP v1	• Modifica l'origine dati e disattiva le prestazioni dello switch • Modifica l'origine dati e la configurazione dello switch per utilizzare SNMP v2 o superiore

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Cohesity SmartFiles

Questo collettore basato su API REST acquisirà un cluster Cohesity, scoprendo le "Visualizzazioni" (come volumi interni Data Infrastructure Insights), i vari nodi e raccogliendo metriche sulle prestazioni.

Configurazione

Campo	Descrizione
IP del cluster Cohesity	Indirizzo IP del cluster Cohesity
Nome utente	Nome utente per il cluster Cohesity
Password	Password utilizzata per il cluster Cohesity

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta utilizzata per la comunicazione TCP con il cluster Cohesity
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.
Intervallo di sondaggio sulle prestazioni (min)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 900 secondi.

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Dell

Raccoglitore dati Dell EMC serie XC

Data Infrastructure Insights utilizza questo raccoglitore di dati per scoprire informazioni sull'inventario e sulle prestazioni degli array di storage Dell EMC XC Series.

Configurazione

Campo	Descrizione
Indirizzo IP esterno Prism	Indirizzo IP del server XC
Nome utente	Nome utente per il server XC
Password	Password utilizzata per il server XC

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta utilizzata per la comunicazione TCP con il server XC
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.
Intervallo di sondaggio sulle prestazioni (min)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Dell EMC

Raccoglitore dati DELL EMC Data Domain

Questo raccoglitore di dati raccoglie informazioni sull'inventario e sulle prestazioni dai sistemi di storage di deduplicazione DELL EMC Data Domain. Per configurare questo raccoglitore di dati, è necessario seguire specifiche istruzioni di configurazione e raccomandazioni d'uso.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Data Domain. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Vettore	Magazzinaggio
Porto FC	Porta
Sistema di file	Volume interno
Quota	Quota
Condivisione NFS e CIFS	Condivisione file

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni:

- Indirizzo IP del dispositivo Data Domain
- Nome utente e password di sola lettura per l'archiviazione Data Domain
- Porta SSH 22

Configurazione

Campo	Descrizione
indirizzo IP	L'indirizzo IP o il nome di dominio completo dell'array di archiviazione Data Domain
Nome utente	Il nome utente per l'array di archiviazione Data Domain
Password	La password per l'array di archiviazione Data Domain

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20.
Porta SSH	Porta del servizio SSH

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati EMC ECS

Questo raccoglitore di dati acquisisce dati di inventario e prestazioni dai sistemi di storage EMC ECS. Per la configurazione, il raccoglitore dati richiede un indirizzo IP o un nome host del cluster ECS, nonché un nome utente e una password.

Dell EMC ECS viene misurato a una tariffa Raw TB diversa da quella delle unità gestite. Ogni 40 TB di capacità ECS non formattata viene addebitato come 1"Unità gestita (MU)" .

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati ECS. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per tale asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Grappolo	Magazzinaggio
Inquilino	Pool di archiviazione
Secchio	Volume interno
Disco	Disco

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Un indirizzo IP o un nome host del cluster ECS
- Un nome utente e una password per il sistema ECS
- Porta 4443 (HTTPS). Richiede connettività in uscita alla porta TCP 4443 sul sistema ECS.

Configurazione

Campo	Descrizione
ECS Host	Indirizzo IP o nome di dominio completo del sistema ECS
Porta host ECS	Porta utilizzata per la comunicazione con l'host ECS
ID utente ECS	ID utente per ECS
Password	Password utilizzata per ECS

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 360 minuti.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: autenticazione utente fallita.	Assicurati che le credenziali per questo dispositivo siano corrette.

Prestazione

Problema:	Prova questo:
Errore: non sono stati raccolti dati sufficienti.	* Controllare il timestamp della raccolta nel file di registro e modificare di conseguenza l'intervallo di polling * Attendere un tempo più lungo
Errore: l'intervallo di polling delle prestazioni è troppo grande.	Controllare il timestamp della raccolta nel file di registro ${logfile} e modificare di conseguenza l'intervallo di polling

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Dell EMC PowerScale

Data Infrastructure Insights utilizza il raccoglitore dati SSH Dell EMC PowerScale (in precedenza Isilon) per acquisire dati di inventario e prestazioni dallo storage NAS scalabile PowerScale.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore di dati. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Guidare	Disco
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
Sistema di file	Volume interno

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni:

- Autorizzazioni di amministratore per l'archiviazione PowerScale
- Indirizzo IP del cluster PowerScale
- Accesso SSH alla porta 22

Configurazione

Campo	Descrizione
indirizzo IP	L'indirizzo IP o il nome di dominio completo del cluster PowerScale
Nome utente	Nome utente per il cluster PowerScale
Password	Password utilizzata per il cluster PowerScale

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20.
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300.
Porta SSH	Porta del servizio SSH. Il valore predefinito è 22.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
"Credenziali di accesso non valide" con messaggi di errore "I comandi non abilitati per l'amministrazione basata sui ruoli richiedono l'accesso come utente root"	* Verificare che l'utente abbia le autorizzazioni per eseguire i seguenti comandi sul dispositivo: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verificare che le credenziali utilizzate nella procedura guidata corrispondano alle credenziali del dispositivo
"Errore interno" con messaggi di errore "Esecuzione del comando <Il tuo comando> non riuscita con autorizzazione: <La tua autorizzazione attuale>. Problema con l'autorizzazione all'esecuzione del comando Sudo"	Verificare che l'utente abbia i permessi sudo per eseguire il seguente comando sul dispositivo

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati REST Dell EMC Isilon / PowerScale

Data Infrastructure Insights utilizza il data collector REST di Dell EMC Isilon/PowerScale per acquisire dati di inventario e prestazioni dallo storage Dell EMC Isilon o PowerScale. Questo collector supporta array che eseguono OneFS 8.0.0+.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore di dati. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Guidare	Disco
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
File system OneFS	Volume interno
File system OneFS	Pool di archiviazione
Qtree	Qtree

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni:

- Un account utente e una password. Questo account NON deve essere necessariamente admin/root, ma DEVI concedere un numero sostanziale di privilegi di sola lettura al tuo account di servizio: vedi tabella qui sotto
- Indirizzo IP / Nome di dominio completo del cluster Dell EMC Isilon / PowerScale

- Accesso HTTPS alla porta 8080
- Cluster Isilon/PowerScale che esegue OneFS 8.0.0 o versione successiva

Nome del privilegio	Descrizione	r(lettura) o rw (lettura+scrittura)
ISI_PRIV_LOGIN_PAPI	API della piattaforma	R
ISI_PRIV_SYS_TIME	Tempo	R
ISI_PRIV_AUTH	Autenticazione	R
ISI_PRIV_RUOLO	Privilegio	R
ISI_PRIV_DEVICES	Dispositivi	R
ISI_PRIV_EVENT	Evento	R
ISI_PRIV_HDFS	HDFS	R
ISI_PRIV_NDMP	NDMP	R
ISI_PRIV_NETWORK	Rete	R
ISI_PRIV_NFS	NFS	R
ISI_PRIV_PAPI_CONFIG	Configurare l'API della piattaforma	R
ISI_PRIV_QUOTA	Quota	R
ISI_PRIV_SMARTPOOLS	Piscine intelligenti	R
ISI_PRIV_SMB	PMI	R
ISI_PRIV_STATISTICS	Statistiche	R
ISI_PRIV_SWIFT	Veloce	R
ISI_PRIV_JOB_ENGINE	Motore di lavoro	R

Configurazione

Campo	Descrizione
Indirizzo IP Isilon	L'indirizzo IP o il nome di dominio completo dello storage Isilon
Nome utente	Nome utente per Isilon
Password	Password utilizzata per Isilon

Configurazione avanzata

Campo	Descrizione
Porta HTTPS	Il valore predefinito è 8080.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20.
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
"Credenziali di accesso non valide" con messaggi di errore "I comandi non abilitati per l'amministrazione basata sui ruoli richiedono l'accesso come utente root"	* Verificare che l'utente abbia le autorizzazioni per eseguire i seguenti comandi sul dispositivo: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verificare che le credenziali utilizzate nella procedura guidata corrispondano alle credenziali del dispositivo
"Errore interno" con messaggi di errore "Esecuzione del comando <Il tuo comando> non riuscita con autorizzazione: <La tua autorizzazione attuale>. Problema con l'autorizzazione all'esecuzione del comando Sudo"	Verificare che l'utente abbia i permessi sudo per eseguire il seguente comando sul dispositivo

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Dell EMC PowerStore

Il raccoglitore dati EMC PowerStore raccoglie informazioni di inventario dallo storage EMC PowerStore. Per la configurazione, il raccoglitore dati richiede l'indirizzo IP dei processori di archiviazione e un nome utente e una password di sola lettura.

Il raccoglitore dati EMC PowerStore raccoglie le relazioni di replica da volume a volume che PowerStore coordina tra altri array di storage. Data Infrastructure Insights mostra un array di archiviazione per ogni cluster PowerStore e raccoglie i dati di inventario per i nodi e le porte di archiviazione su quel cluster. Non vengono raccolti dati di pool di archiviazione o di volume.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore di dati. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
ospite	ospite
host_volume_mapping	host_volume_mapping
hardware (ha Unità sotto l'oggetto "extra_details"): Unità	Disco
Apparecchio	StoragePool
Grappolo	Array di archiviazione
Nodo	StorageNode

Termine del fornitore/modello	Termine Data Infrastructure Insights
fc_port	Porta
volume	Volume
Volume interno	file system

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni:

- Indirizzo IP o nome di dominio completo del processore di archiviazione
- Nome utente e password di sola lettura

Configurazione

Campo	Descrizione
Gateway PowerStore	Indirizzi IP o nomi di dominio completi dello storage PowerStore
Nome utente	Nome utente per PowerStore
Password	Password utilizzata per PowerStore

Configurazione avanzata

Campo	Descrizione
Porta HTTPS	Il valore predefinito è 443
Intervallo di sondaggio dell'inventario (minuti)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.

La raccolta delle prestazioni di PowerStore di Cloud Insight sfrutta i dati sorgente con granularità di 5 minuti di PowerStore. Pertanto, Data Infrastructure Insights esegue il polling di tali dati ogni cinque minuti e questa operazione non è configurabile.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Dell EMC RecoverPoint

Il caso d'uso principale del raccoglitore dati EMC RecoverPoint è quello di scoprire le relazioni di replica tra volumi facilitate dall'appliance di storage RecoverPoint. Questo raccoglitore scoprirà anche l'appliance Recoverpoint stessa. Si prega di notare che Dell/EMC vende una soluzione di backup VMware per VM, "RecoverPoint for VMs", che non è supportata da questo collector.

Per la configurazione, il raccoglitore dati richiede l'indirizzo IP dei processori di archiviazione e un nome utente e una password di sola lettura.

Il raccoglitore dati EMC RecoverPoint raccoglie le relazioni di replica da volume a volume che RecoverPoint coordina tra altri array di storage. Data Infrastructure Insights mostra un array di archiviazione per ogni cluster RecoverPoint e raccoglie i dati di inventario per i nodi e le porte di archiviazione su quel cluster. Non vengono raccolti dati di pool di archiviazione o di volume.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni:

- Indirizzo IP o nome di dominio completo del processore di archiviazione
- Nome utente e password di sola lettura
- Accesso API REST tramite porta 443

Configurazione

Campo	Descrizione
Indirizzo di RecoverPoint	Indirizzo IP o nome di dominio completo del cluster RecoverPoint
Nome utente	Nome utente per il cluster RecoverPoint
Password	Password utilizzata per il cluster RecoverPoint

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per connettersi al cluster Recoverpoint
Intervallo di sondaggio dell'inventario (minuti)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20 minuti.
Cluster esclusi	Elenco separato da virgole di ID o nomi di cluster da escludere durante il polling.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati DELL EMC ScaleIO / PowerFlex

Il raccoglitore dati ScaleIO/PowerFlex raccoglie informazioni di inventario dallo storage ScaleIO e PowerFlex. Per la configurazione, questo raccoglitore dati richiede l'indirizzo del gateway ScaleIO/PowerFlex e un nome utente e una password amministratore.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati ScaleIO/PowerFlex. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la

terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Cluster MDM (Meta Data Manager)	Magazzinaggio
SDS (server dati ScaleIO/PowerFlex)	Nodo di archiviazione
Pool di archiviazione	Pool di archiviazione
Volume	Volume
Dispositivo	Disco

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Accesso di sola lettura all'account utente amministratore
- Requisito porta: Porta HTTPS 443

Configurazione

Campo	Descrizione
Gateway ScaleIO/PowerFlex	Indirizzi IP o FQDN dei gateway ScaleIO/PowerFlex, separati da virgola (,) o punto e virgola (;)
Nome utente	Nome utente amministratore utilizzato per accedere al dispositivo ScaleIO/PowerFlex
Password	Password utilizzata per accedere al dispositivo ScaleIO/PowerFlex

Configurazione avanzata

Fare clic sulla casella di controllo Inventario per abilitare la raccolta dell'inventario.

Campo	Descrizione
Porta HTTPS	443
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60.
Timeout di connessione (sec)	Il valore predefinito è 60.

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati EMC Unity

Il raccoglitore dati DELL EMC Unity (in precedenza VNXe) fornisce supporto di inventario per gli array di storage unificati VNXe. Data Infrastructure Insights supporta attualmente i

protocolli iSCSI e NAS.

Requisiti

- Il data collector Unity è basato sulla CLI; è necessario installare Unisphere per Unity CLI (uemcli.exe) sull'unità di acquisizione in cui risiede il data collector VNXe.
- uemcli.exe utilizza HTTPS come protocollo di trasporto, pertanto l'unità di acquisizione dovrà essere in grado di avviare connessioni HTTPS a Unity.
- Indirizzo IP o nome di dominio completo del dispositivo Unity
- Per l'utilizzo da parte del raccoglitore dati è necessario disporre almeno di un utente con privilegi di sola lettura.
- È richiesto HTTPS sulla porta 443
- Il data collector EMC Unity fornisce supporto NAS e iSCSI per l'inventario; i volumi Fibre Channel verranno rilevati, ma Data Infrastructure Insights non fornisce report sulla mappatura FC, sul mascheramento o sulle porte di archiviazione.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Unity. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Array di archiviazione	Magazzinaggio
Processore	Nodo di archiviazione
Pool di archiviazione	Pool di archiviazione
Informazioni generali sul blocco iSCSI, VMware VMFS	Condividere
Sistema remoto di replicazione	Sincronizzazione
Nodo iSCSI	Nodo di destinazione iSCSI
Iniziatore iSCSI	Iniziatore di destinazione iSCSI

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa fonte dati.

Configurazione

Campo	Descrizione
Unity Storage	Indirizzo IP o nome di dominio completo del dispositivo Unity
Nome utente	Nome utente per il dispositivo Unity
Password	Password per il dispositivo Unity

Campo	Descrizione
Percorso completo dell'eseguibile UEMCLI	Percorso completo della cartella contenente l'eseguibile *uemcli.exe*

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti
Porta CLI Unity	Porta utilizzata per Unity CLI
Intervallo di sondaggio delle prestazioni (sec)	Il valore predefinito è 300.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
"Impossibile eseguire l'utilità esterna" con messaggi di errore "Impossibile trovare l'eseguibile Unisphere uemcli"	* Verificare la correttezza dell'indirizzo IP, del nome utente e della password. * Confermare che Unisphere CLI sia installato sull'unità di acquisizione Data Infrastructure Insights. * Confermare che la directory di installazione di Unisphere CLI sia corretta nella configurazione dell'origine dati. * Confermare che l'IP del VNXe sia corretto nella configurazione dell'origine dati. Dall'unità di acquisizione Data Infrastructure Insights , aprire un CMD e passare alla directory di installazione configurata: ${INSTALLDIR. Prova a stabilire una connessione con il dispositivo VNXe digitando: uemcli -d <Il tuo IP> -u <Il tuo ID> /sys/general show

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati della famiglia di dispositivi Dell EMC VMAX e PowerMax

Data Infrastructure Insights rileva gli array di storage EMC VMAX e PowerMax utilizzando i comandi symcli di Solutions Enabler insieme a un server Solutions Enabler esistente nel tuo ambiente. Il server Solutions Enabler esistente è dotato di connettività con l'array di storage VMAX/PowerMax tramite l'accesso ai volumi gatekeeper.

Requisiti

Prima di configurare questo raccoglitore dati, è necessario assicurarsi che Data Infrastructure Insights disponga di connettività TCP sulla porta 2707 sul server Solutions Enabler esistente. Data Infrastructure Insights rileva tutti gli array Symmetrix che sono "locali" per questo server, come mostrato nell'output "symcfg list" da quel server.

- L’applicazione provider EMC Solutions Enabler (CLI) con SMI-S deve essere installata sul server Acquisition Unit e la versione deve corrispondere o essere precedente alla versione in esecuzione sul server Solutions Enabler.
- È necessario un file {installdir}\EMC\SYMAPI\config\netcnfg configurato correttamente. Questo file definisce i nomi dei servizi per i server Solutions Enabler, nonché il metodo di accesso (SECURE / NOSECURE /ANY).
- Se è necessaria una latenza di lettura/scrittura a livello di nodo di archiviazione, il provider SMI-S deve comunicare con un’istanza in esecuzione dell’applicazione UNISPHERE for VMAX.
- Indirizzo IP del server Solutions Enabler di gestione
- Autorizzazioni di amministratore sul server Solutions Enabler (SE)
- Nome utente e password di sola lettura per il software SE
- L’applicazione UNISPHERE per VMAX deve essere in esecuzione e raccogliere statistiche per gli array di storage EMC VMAX e PowerMax gestiti dall’installazione del provider SMI-S
- Convalida dell’accesso per le prestazioni: in un browser Web sulla tua unità di acquisizione, vai a *https://<Nome host o IP SMI-S>:5989/ecomconfig* dove "Nome host o IP SMI-S" è l’indirizzo IP o il nome host del tuo server SMI-S. Questo URL è per un portale amministrativo per il servizio EMC SMI-S (noto anche come "ECOM"): riceverai una finestra popup di accesso.
- Le autorizzazioni devono essere dichiarate nel file di configurazione del daemon del server Solutions Enabler, solitamente reperibile qui: */var/symapi/config/daemon_users*

  Ecco un file di esempio con le autorizzazioni cisys appropriate.

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
##############################################################################
########
# smith         storrdfd
cisys storapid <all>
```

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dalla fonte dati EMC VMAX/PowerMax. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per tale asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Gruppo di dischi	Gruppo di dischi

Termine del fornitore/modello	Termine Data Infrastructure Insights
Magazzinaggio	Archiviazione array
Direttore	Nodo di archiviazione
Pool di dispositivi, pool di risorse di archiviazione (SRP)	Pool di archiviazione
Dispositivo TDev	Volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Configurazione

Nota: se l'autenticazione utente SMI-S non è abilitata, i valori predefiniti nel raccoglitore Data Infrastructure Insights vengono ignorati.

Campo	Descrizione
Nome del servizio	Nome del servizio come specificato nel file *netcnfg*
Percorso completo alla CLI	Percorso completo della cartella contenente Symmetrix CLI
Indirizzo IP host SMI-S	Indirizzo IP dell'host SMI-S

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti.
Selezionare "Escludi" o "Includi" per specificare un elenco	Specificare se includere o escludere l'elenco di array sottostante durante la raccolta dei dati.
Elenco dispositivi filtro inventario	Elenco separato da virgole di ID dispositivo da includere o escludere

Campo	Descrizione
Caching delle connessioni	Selezionare il metodo di memorizzazione nella cache della connessione: * LOCALE significa che il servizio Cloud Insights Acquisition è in esecuzione sul server Solutions Enabler, che dispone di connettività Fibre Channel con gli array Symmetrix che si desidera individuare e ha accesso ai volumi gatekeeper. Ciò potrebbe verificarsi in alcune configurazioni di unità di acquisizione remota (RAU). * REMOTE_CACHED è l'impostazione predefinita e dovrebbe essere utilizzata nella maggior parte dei casi. In questo modo vengono utilizzate le impostazioni del file NETCNFG per connettersi tramite IP al server Solutions Enabler, che deve disporre di connettività Fibre Channel con gli array Symmetrix che si desidera rilevare e avere accesso ai volumi Gatekeeper. * Nel caso in cui le opzioni REMOTE_CACHED facciano fallire i comandi CLI, utilizzare l'opzione REMOTE. Tieni presente che ciò rallenterà il processo di acquisizione (potenzialmente di ore o addirittura giorni nei casi estremi). Le impostazioni del file NETCNFG vengono ancora utilizzate per una connessione IP al server Solutions Enabler dotato di connettività Fibre Channel con gli array Symmetrix rilevati. **Nota:** questa impostazione non modifica il comportamento Data Infrastructure Insights rispetto agli array elencati come REMOTE dall'output "symcfg list". Data Infrastructure Insights raccoglie dati solo sui dispositivi indicati come LOCALI da questo comando.
Protocollo SMI-S	Protocollo utilizzato per connettersi al provider SMI-S. Visualizza anche la porta predefinita utilizzata.
Sostituisci SMIS-Port	Se vuoto, utilizzare la porta predefinita nel campo Tipo di connessione, altrimenti immettere la porta di connessione da utilizzare
Nome utente SMI-S	Nome utente per l'host del provider SMI-S
Password SMI-S	Nome utente per l'host del provider SMI-S
Intervallo di polling delle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni (predefinito 1000 secondi)
Scegli "Escludi" o "Includi" per specificare un elenco	Specificare se includere o escludere l'elenco di array sottostante durante la raccolta dei dati sulle prestazioni
Elenco dispositivi filtro prestazioni	Elenco separato da virgole di ID dispositivo da includere o escludere

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Problema:	Prova questo:
Errore: la funzionalità richiesta non è attualmente concessa in licenza	Installare la licenza del server SYMAPI.
Errore: nessun dispositivo trovato	Assicurarsi che i dispositivi Symmetrix siano configurati per essere gestiti dal server Solutions Enabler: - Eseguire symcfg list -v per visualizzare l'elenco dei dispositivi Symmetrix configurati.
Errore: il servizio di rete richiesto non è stato trovato nel file di servizio	Assicurarsi che il nome del servizio Solutions Enabler sia definito nel file netcnfg per Solutions Enabler. Questo file si trova solitamente in SYMAPI\config\ nell'installazione del client Solutions Enabler.
Errore: l'handshake client/server remoto non è riuscito	Controllare i file storsrvd.log* più recenti sull'host Solutions Enabler che stiamo cercando di individuare.
Errore: nome comune nel certificato client non valido	Modificare il file *hosts* sul server Solutions Enabler in modo che il nome host dell'unità di acquisizione venga risolto nell'indirizzo IP riportato nel file storsrvd.log sul server Solutions Enabler.
Errore: la funzione non è riuscita a ottenere memoria	Assicurarsi che ci sia abbastanza memoria libera disponibile nel sistema per eseguire Solutions Enabler
Errore: Solutions Enabler non è riuscito a fornire tutti i dati richiesti.	Esaminare lo stato di salute e il profilo di carico di Solutions Enabler
Errore: • Il comando CLI "symcfg list -tdev" potrebbe restituire dati non corretti quando raccolti con Solutions Enabler 7.x da un server Solutions Enabler 8.x. • Il comando CLI "symcfg list -srp" potrebbe restituire dati non corretti se raccolti con Solutions Enabler 8.1.0 o versioni precedenti da un server Solutions Enabler 8.3 o versioni successive.	Assicurati di utilizzare la stessa versione principale di Solutions Enabler
Vedo errori di raccolta dati con il messaggio: "codice sconosciuto"	Questo messaggio potrebbe essere visualizzato se le autorizzazioni non sono dichiarate nel file di configurazione del daemon del server Solutions Enabler (vedereRequisiti Sopra.) Ciò presuppone che la versione del client SE corrisponda alla versione del server SE. Questo errore può verificarsi anche se l'utente *cisys* (che esegue i comandi Solutions Enabler) non è stato configurato con le autorizzazioni daemon necessarie nel file di configurazione /var/symapi/config/daemon_users. Per risolvere questo problema, modifica il file /var/symapi/config/daemon_users e assicurati che l'utente cisys abbia specificato l'autorizzazione <all> per il demone storapid. Esempio: 14:11:25 # tail /var/symapi/config/daemon_users … cisys storapid <all>

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Dell EMC VNX Block Storage (NaviCLI)

Data Infrastructure Insights utilizza il raccoglitore dati Dell EMC VNX Block Storage (NaviSec) (in precedenza CLARiiON) per acquisire dati di inventario e prestazioni.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal data collector EMC VNX Block Storage. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Magazzinaggio	Magazzinaggio
Processore di archiviazione	Nodo di archiviazione
Questo pool, gruppo RAID	Pool di archiviazione
LUN	Volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa fonte dati.

Requisiti

Per poter raccogliere i dati è necessario soddisfare i seguenti requisiti:

- Un indirizzo IP di ciascun processore di archiviazione a blocchi VNX
- Nome utente e password Navisphere di sola lettura per gli array di archiviazione a blocchi VNX
- NaviSecCli deve essere installato su Data Infrastructure Insights AU
- Convalida dell'accesso: eseguire NaviSecCLI da Data Infrastructure Insights AU su ciascun array utilizzando il nome utente e la password.
- Requisiti della porta: 80, 443
- La versione di NaviSecCLI dovrebbe corrispondere al codice FLARE più recente sul tuo array
- Per migliorare le prestazioni, è necessario abilitare la registrazione delle statistiche.

Sintassi dell'interfaccia della riga di comando di NaviSphere

naviseccli.exe -h <indirizzo IP> -user <utente> -password <password> -scope <ambito, usa 0 per l'ambito globale> -port <usa 443 per impostazione predefinita> comando

Configurazione

Campo	Descrizione
Indirizzo IP di archiviazione a blocchi VNX	Indirizzo IP o nome di dominio completo dell'archiviazione a blocchi VNX
Nome utente	Nome utilizzato per accedere al dispositivo di archiviazione a blocchi VNX.

Campo	Descrizione
Password	Password utilizzata per accedere al dispositivo di archiviazione a blocchi VNX.
Percorso CLI per naviseccli.exe	Percorso completo della cartella contenente l'eseguibile *naviseccli.exe*

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti.
Ambito	Ambito client sicuro. L'impostazione predefinita è Globale.
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: • Agente non in esecuzione • Impossibile trovare naviseccli • Impossibile eseguire alcun comando	• Verificare che NaviSphere CLI sia installato su Cloud Insight Acquisition Unit • Non hai selezionato l'opzione "Usa client sicuro" nella procedura guidata di configurazione del raccoglitore dati e non hai installato una versione non sicura di Naviphere CLI. • Verificare che la directory di installazione di NaviSphere CLI sia corretta nella configurazione del raccoglitore dati • Verificare che l'IP dell'archiviazione a blocchi VNX sia corretto nella configurazione del raccoglitore dati: • Dall'unità di acquisizione Data Infrastructure Insights : ◦ Aprire un CMD. ◦ Cambiare la directory nella directory di installazione configurata ◦ Prova a stabilire una connessione con il dispositivo di archiviazione a blocchi VNX digitando "navicli -h {ip} getagent" (sostituisci {ip} con l'IP effettivo)

Problema:	Prova questo:
Errore: 4.29 emc235848 emc241018 getall Impossibile analizzare le informazioni sull'alias dell'host	Ciò è probabilmente causato da un problema di danneggiamento FLARE 29 del database dell'iniziatore host sull'array stesso. Vedere gli articoli della knowledge base EMC: emc235848, emc241018. Puoi anche controllare https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Errore: impossibile recuperare i Meta LUN. Errore durante l'esecuzione di java -jar navicli.jar	• Modificare la configurazione del raccoglitore dati per utilizzare il client sicuro (consigliato) • Installare navicli.jar nel percorso CLI per navicli.exe O naviseccli.exe • Nota: navicli.jar è obsoleto a partire dalla versione 6.26 di EMC Navisphere • Il file navicli.jar potrebbe essere disponibile su \ http://powerlink.emc.com
Errore: i pool di archiviazione non segnalano i dischi sul processore di servizio all'indirizzo IP configurato	Configurare il raccoglitore dati con entrambi gli IP del processore di servizio, separati da una virgola
Errore: errore di mancata corrispondenza della revisione	• In genere, ciò è causato dall'aggiornamento del firmware sul dispositivo di archiviazione a blocchi VNX, ma non dall'aggiornamento dell'installazione di NaviCLI.exe. Ciò potrebbe essere causato anche dalla presenza di dispositivi diversi con firmware diversi, ma di una sola CLI installata (con una versione firmware diversa). • Verificare che sia il dispositivo che l'host eseguano versioni identiche del software: ◦ Dall'unità di acquisizione Data Infrastructure Insights , aprire una finestra della riga di comando ◦ Cambiare la directory nella directory di installazione configurata ◦ Stabilisci una connessione con il dispositivo CLARiiON digitando "navicli -h <ip> getagent" ◦ Cerca il numero di versione nelle prime due righe. Esempio: "Agente Rev: 6.16.2 (0.1)" ◦ Cerca e confronta la versione sulla prima riga. Esempio: "Navisphere CLI Revisione 6.07.00.04.07"
Errore: configurazione non supportata - nessuna porta Fibre Channel	Il dispositivo non è configurato con alcuna porta Fibre Channel. Attualmente sono supportate solo le configurazioni FC. Verificare che questa versione/firmware sia supportata.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati DELL EMC VNX File (in precedenza Celerra Unified Storage System)

Questo raccoglitore di dati acquisisce informazioni di inventario dal sistema di archiviazione file VNX. Per la configurazione, questo raccoglitore di dati richiede l'indirizzo IP dei processori di archiviazione e un nome utente e una password di sola lettura.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati VNX File. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Server di rete Celerra/pool di archiviazione Celerra	Pool di archiviazione
Sistema di file	Volume interno
Spostamento dati	Controllore
File System montato su un data mover	Condivisione file
Esportazioni CIFS e NFS	Condividere
Volume del disco	LUN di backend

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati è necessario quanto segue:

- L'indirizzo IP del processore di archiviazione
- Nome utente e password di sola lettura
- Porta SSH 22

Configurazione

Campo	Descrizione
Indirizzo IP del file VNX	Indirizzo IP o nome di dominio completo del dispositivo file VNX
Nome utente	Nome utilizzato per accedere al dispositivo VNX File
Password	Password utilizzata per accedere al dispositivo VNX File

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (minuti)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20 minuti.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: impossibile procedere mentre è in corso l'aggiornamento DART	Soluzione possibile: mettere in pausa il raccoglitore dati e attendere il completamento dell'aggiornamento DART prima di tentare un'altra richiesta di acquisizione.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del data collector Dell EMC VNX Unified

Per la configurazione, il data collector Dell EMC VNX Unified (SSH) richiede l'indirizzo IP della Control Station e un nome utente e una password di sola lettura.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore di dati. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Cartella del disco	Gruppo di dischi
Sistema di file	Volume interno
Magazzinaggio	Magazzinaggio
Processore di archiviazione	Nodo di archiviazione
Pool di archiviazione, gruppo RAID	Pool di archiviazione
LUN	Volume
Spostamento dati	Controllore
File System montato su un data mover	Condivisione file
Esportazioni CIFS e NFS	Condividere
Volume del disco	LUN di backend

Requisiti

Per configurare il raccoglitore dati VNX (SSH) è necessario quanto segue:

- Indirizzo IP VNX e credenziali per la stazione di controllo Celerra.
- Nome utente e password di sola lettura.
- Il raccoglitore di dati è in grado di eseguire comandi NaviCLI/NaviSecCLI sull'array backend utilizzando le testine NAS del sistema operativo DART

Configurazione

Campo	Descrizione
Indirizzo IP VNX	Indirizzo IP o nome di dominio completo della stazione di controllo VNX
Nome utente	Nome utente per la stazione di controllo VNX
Password	Password per la stazione di controllo VNX

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti.
Intervallo di sondaggio sulle prestazioni (sec).	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati EMC VPLEX

Questo raccoglitore di dati acquisisce dati di inventario e prestazioni dai sistemi di storage EMC VPLEX. Per la configurazione, il raccoglitore dati necessita di un indirizzo IP del server VPLEX e di un account di dominio di livello amministrativo.

Per poter raccogliere dati sulle prestazioni di Data Infrastructure Insights dai cluster Vplex, è necessario che il servizio di archiviazione delle prestazioni sia operativo, per popolare i file .CSV e i log che Data Infrastructure Insights recupera tramite copie di file basate su SCP. NetApp ha osservato che molti aggiornamenti del firmware/della stazione di gestione Vplex renderanno questa funzionalità non operativa. I clienti che pianificano tali aggiornamenti potrebbero voler chiedere in modo proattivo a Dell/EMC se l'aggiornamento pianificato renderà questa funzionalità inutilizzabile e, in tal caso, come possono riattivarla per ridurre al minimo le lacune nella visibilità delle prestazioni? Il codice delle prestazioni Vplex di Cloud Insight valuterà a ogni polling se tutti i file previsti esistono e se vengono aggiornati correttamente; se sono mancanti o obsoleti, Data Infrastructure Insights registrerà gli errori di raccolta delle prestazioni.

Terminologia

Data Infrastructure Insightst acquisisce le seguenti informazioni di inventario dal raccoglitore dati VPLEX. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per tale asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Grappolo	Magazzinaggio
Motore	Nodo di archiviazione
Dispositivo, estensione del sistema	Pool di archiviazione back-end
Volume virtuale	Volume
Porta front-end, porta back-end	Porta
Dispositivo distribuito	Sincronizzazione dell'archiviazione
Vista di archiviazione	Mappa del volume, maschera del volume
Volume di archiviazione	LUN di backend
ITL	Percorso backend

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Un indirizzo IP della console di gestione VPLEX
- Account di dominio a livello amministrativo per il server VPLEX
- Porta 443 (HTTPS). Richiede connettività in uscita alla porta TCP 443 sulla stazione di gestione VPLEX.
- Per migliorare le prestazioni, nome utente e password di sola lettura per l'accesso ssh/scp.
- Per le prestazioni è richiesta la porta 22.

Configurazione

Campo	Descrizione
Indirizzo IP della console di gestione VPLEX	Indirizzo IP o nome di dominio completo della console di gestione VPLEX
Nome utente	Nome utente per VPLEX CLI
Password	Password utilizzata per VPLEX CLI
Indirizzo IP remoto delle prestazioni	Indirizzo IP remoto delle prestazioni della console di gestione VPLEX
Nome utente remoto delle prestazioni	Nome utente remoto delle prestazioni della console di gestione VPLEX
Password remota per le prestazioni	Password remota delle prestazioni della console di gestione VPLEX

Configurazione avanzata

Campo	Descrizione
Porta di comunicazione	Porta utilizzata per VPLEX CLI. Il valore predefinito è 443.
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 20 minuti.
Numero di tentativi di connessione	Il valore predefinito è 3.
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 600 secondi.
Numero di tentativi	Il valore predefinito è 2.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: autenticazione utente fallita.	Assicurati che le credenziali per questo dispositivo siano corrette.

Prestazione

Problema:	Prova questo:
Errore: le prestazioni di VPLEX per la versione precedente alla 5.3 non sono supportate.	Aggiorna VPLEX alla versione 5.3 o successiva
Errore: non sono stati raccolti dati sufficienti.	• Controllare il timestamp della raccolta nel file di registro e modificare di conseguenza l'intervallo di polling • Attendere un tempo più lungo
Errore: i file di registro perpetui non vengono aggiornati.	Contattare il supporto EMC per abilitare l'aggiornamento dei file di registro perpetui
Errore: l'intervallo di polling delle prestazioni è troppo grande.	Controllare il timestamp della raccolta nel file di registro ${logfile} e modificare di conseguenza l'intervallo di polling
Errore: l'indirizzo IP remoto delle prestazioni della console di gestione VPLEX non è configurato.	Modificare l'origine dati per impostare l'indirizzo IP remoto delle prestazioni della console di gestione VPLEX.
Errore: nessun dato sulle prestazioni segnalato dal direttore	• Verificare che i monitor delle prestazioni del sistema funzionino correttamente • Contattare il supporto EMC per abilitare l'aggiornamento dei file di registro del monitor delle prestazioni del sistema

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Dell EMC XtremeIO

Il raccoglitore dati EMC XtremIO acquisisce dati di inventario e prestazioni dal sistema di storage EMC XtremIO.

Requisiti

Per configurare il raccoglitore dati EMC XtremIO (HTTP), è necessario disporre di:

- Indirizzo host del server di gestione XtremIO (XMS)
- Un account con privilegi di amministratore
- Accesso alla porta 443 (HTTPS)

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati EMC XtremIO. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema relativo a questa origine dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco (SSD)	Disco
Grappolo	Magazzinaggio
Controllore	Nodo di archiviazione
Volume	Volume
Mappa LUN	Mappa del volume
Iniziatore FC target	Maschera del volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa fonte dati.

Requisiti

- Indirizzo IP dell'host del server di gestione XtremIO (XMS)
- Nome utente e password dell'amministratore per XtremIO

Configurazione

Campo	Descrizione
Host XMS	Indirizzo IP o nome di dominio completo del server di gestione XtremIO
Nome utente	Nome utente per XtremIO Management Server
Password	Password per il server di gestione XtremIO

Configurazione avanzata

Campo	Descrizione
porta TCP	Porta TCP utilizzata per connettersi al server di gestione XTremIO. Il valore predefinito è 443.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.
Intervallo di sondaggio delle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Fujitsu Eternus

Il raccoglitore dati Fujitsu Eternus acquisisce i dati di inventario utilizzando l'accesso a livello di amministrazione al sistema di archiviazione.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dallo storage Fujitsu Eternus. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Magazzinaggio	Magazzinaggio
Pool sottile, pool di livelli flessibile, gruppo raid	Pool di archiviazione
Volume standard, volume dati Snap (SDV), volume pool dati Snap (SDPV), volume thin provisioning (TPV), volume livello flessibile (FTV), volume wide striping (WSV)	Volume
Adattatore di canale	Controllore

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessari i seguenti elementi:

- Un indirizzo IP dello storage Eternus, che non può essere delimitato da virgole
- Nome utente e password di livello di amministrazione SSH
- Porta 22
- Assicurarsi che lo scorrimento della pagina sia disabilitato (clienv-show-more-scroll disable)

Configurazione

Campo	Descrizione
Indirizzo IP di Eternus Storage	Indirizzo IP dello storage Eternus
Nome utente	Nome utente per l'archiviazione Eternus
Password	Password per l'archiviazione Eternus

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 20 minuti.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
"Errore durante il recupero dei dati" con messaggi di errore "Errore durante la ricerca del prompt CLI" o "Errore durante la ricerca del prompt alla fine dei risultati della shell"	Probabilmente causato da: il sistema di archiviazione ha lo scorrimento delle pagine abilitato. Possibile soluzione: * Provare a disabilitare lo scorrimento della pagina eseguendo il seguente comando: set clienv-show-more -scroll disable
"Errore di connessione" con messaggi di errore "Impossibile creare un'istanza di una connessione SSH allo storage" o "Impossibile creare un'istanza di una connessione a VirtualCenter"	Probabili cause: * Credenziali errate. * Indirizzo IP errato. * Problema di rete. * Lo storage potrebbe essere inattivo o non rispondere. Possibili soluzioni: * Verificare le credenziali e l'indirizzo IP immessi. * Prova a comunicare con l'archiviazione utilizzando il client SSH.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati NetApp Google Compute

Questo raccoglitore di dati supporta la raccolta di inventario e prestazioni dalle configurazioni della piattaforma cloud di Google Compute. Questo raccoglitore cercherà di scoprire tutte le risorse di calcolo all'interno di tutti i progetti all'interno di un'organizzazione Google. Se desideri scoprire più organizzazioni Google con Data Infrastructure Insights, dovrai distribuire un raccoglitore Data Infrastructure Insights per organizzazione.

Requisiti dell'account di servizio

- È necessario creare un account di servizio seguendo le istruzioni in"Creazione/gestione di account di servizio" . Tale account di servizio è identificato da un ID univoco, noto come *clientId*, che verrà utilizzato come nome utente.

- Inoltre, crea una chiave dell'account di servizio seguendo le istruzioni in"Creazione/gestione delle chiavi dell'account di servizio" . Questa chiave può essere scaricata come file json, il cui contenuto verrà utilizzato come password.
- L'account di servizio deve avere come ambito *compute.readonly*, *monitoring.read* e *cloud-platform*.

Configurazione

Campo	Descrizione
ID organizzazione	L'ID dell'organizzazione che vuoi scoprire con questo raccoglitore. Questo campo è obbligatorio se il tuo account di servizio è in grado di vedere più di un'organizzazione
Seleziona "Escludi" o "Includi" per filtrare i progetti GCP in base agli ID	Se si desidera limitare le risorse dei progetti che vengono importate in Data Infrastructure Insights.
ID progetto	Elenco degli ID progetto che si desidera filtrare all'interno o all'esterno dell'individuazione, a seconda del valore "Scegli 'Escludi'…". L'elenco predefinito è vuoto
ID cliente	ID client per la configurazione di Google Cloud Platform
Copia e incolla qui il contenuto del tuo file delle credenziali di Google	Copia le tue credenziali Google per l'account Cloud Platform in questo campo

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti
Scegli "Escludi" o "Includi" per applicare il filtro alle VM in base alle etichette	Specificare se includere o escludere le VM in base alle etichette durante la raccolta dei dati. Se è selezionato "Includi", il campo Chiave etichetta non può essere vuoto.
Etichettare le chiavi e i valori in base ai quali filtrare le VM	Fare clic su **+ Etichetta filtro** per scegliere quali VM (e dischi associati) includere/escludere filtrando le chiavi e i valori che corrispondono alle chiavi e ai valori delle etichette sulla VM. La chiave dell'etichetta è obbligatoria, il valore dell'etichetta è facoltativo. Quando il valore dell'etichetta è vuoto, la macchina virtuale viene filtrata finché corrisponde alla chiave dell'etichetta.
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 1800 secondi

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Google Cloud NetApp Volumes

Questo raccoglitore di dati supporta la raccolta di inventario e prestazioni dalle configurazioni Google Cloud NetApp Volumes . Il raccoglitore rileva i volumi NetApp e le risorse di archiviazione in tutti i progetti all'interno di un'organizzazione Google. Se desideri monitorare più organizzazioni Google con Data Infrastructure Insights, distribuisci un raccoglitore per organizzazione.

Requisiti dell'account di servizio

- È necessario creare un account di servizio seguendo le istruzioni in"Creazione/gestione di account di servizio" . Questo account di servizio è identificato da un ID univoco, noto come *clientId*, che verrà utilizzato come nome utente.
- Inoltre, crea una chiave dell'account di servizio seguendo le istruzioni in"Creazione/gestione delle chiavi dell'account di servizio" . Questa chiave può essere scaricata come file json, il cui contenuto verrà utilizzato come password.
- L'account di servizio deve avere come ambito *compute.readonly*, *monitoring.read* e *cloud-platform*.

Configurazione

Campo	Descrizione
ID organizzazione	L'ID dell'organizzazione che vuoi scoprire con questo raccoglitore. Questo campo è obbligatorio se il tuo account di servizio è in grado di vedere più di un'organizzazione
Seleziona "Escludi" o "Includi" per filtrare le risorse GCNV in base alla posizione	L'impostazione predefinita è Escludi, poiché questo raccoglitore intende per impostazione predefinita individuare tutti i volumi GCNV in tutto il mondo all'interno della tua organizzazione.
Posizioni di esclusione/inclusione GCNV	Per impostazione predefinita, questo campo è vuoto e viene utilizzato insieme all'opzione "Scegli 'Escludi' o 'Includi'". Se si desidera scoprire risorse solo in determinate regioni, utilizzare queste due opzioni per limitare l'ambito di questo raccoglitore.
ID progetto	Elenco degli ID progetto che si desidera filtrare all'interno o all'esterno dell'individuazione, a seconda del valore "Scegli 'Escludi'…". L'elenco predefinito è vuoto
ID cliente	ID client per la configurazione di Google Cloud Platform
Copia e incolla qui il contenuto del tuo file delle credenziali di Google	Copia le tue credenziali Google per l'account Cloud Platform in questo campo

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti

Campo	Descrizione
Utilizzare il proxy AU per le chiamate API REST	Selezionare questa opzione per fare in modo che il collettore utilizzi lo stesso proxy dell'unità di acquisizione su cui risiede il collettore. Per impostazione predefinita, questa opzione è disabilitata, il che significa che il collettore tenta di inviare chiamate API HTTPS direttamente a Google.
Etichettare le chiavi e i valori in base ai quali filtrare le VM	Fare clic su **+ Etichetta filtro** per scegliere quali VM (e dischi associati) includere/escludere filtrando le chiavi e i valori che corrispondono alle chiavi e ai valori delle etichette sulla VM. La chiave dell'etichetta è obbligatoria, il valore dell'etichetta è facoltativo. Quando il valore dell'etichetta è vuoto, la macchina virtuale viene filtrata finché corrisponde alla chiave dell'etichetta.
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 300 secondi

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

HP Enterprise

Raccoglitore dati HP Enterprise Alletra 9000 / Primera Storage

Data Infrastructure Insights utilizza il raccoglitore dati HP Enterprise Alletra 9000 / HP Enterprise Primera (in precedenza 3PAR) per scoprire inventario e prestazioni.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore di dati. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Campo	Descrizione
Disco fisico	Disco
Sistema di archiviazione	Magazzinaggio
Nodo controller	Nodo di archiviazione
Gruppo di provisioning comune	Pool di archiviazione
Volume virtuale	Volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessari i seguenti elementi:

- Indirizzo IP o FQDN del cluster InServ
- Per l'inventario, nome utente e password di sola lettura per il server StoreServ
- Per le prestazioni, nome utente e password di lettura-scrittura sul server StoreServ
- Requisiti della porta: 22 (raccolta inventario), 5988 o 5989 (raccolta prestazioni) [Nota: le prestazioni sono supportate per StoreServ OS 3.x+]
- Per la raccolta delle prestazioni, verificare che SMI-S sia abilitato effettuando l'accesso all'array tramite SSH.

Configurazione

Campo	Descrizione
Indirizzo IP di archiviazione	Indirizzo IP di archiviazione o nome di dominio completo del cluster StoreServ
Nome utente	Nome utente per il server StoreServ
Password	Password utilizzata per il server StoreServ
Nome utente SMI-S	Nome utente per l'host del provider SMI-S
Password SMI-S	Password utilizzata per l'host del provider SMI-S

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti.
Connettività SMI-S	Protocollo utilizzato per connettersi al provider SMI-S
Sostituisci la porta predefinita SMI-S	Se vuoto, utilizzare la porta predefinita da SMI-S Connectivity, altrimenti immettere la porta di connessione da utilizzare
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Il comando "showsys" non restituisce alcun risultato.	Eseguire "showsys" e "showversion -a" dalla riga di comando e verificare se la versione è supportata dall'array.

Prestazione

Problema:	Prova questo:
Impossibile connettersi o effettuare l'accesso. Inizializzazione del provider non riuscita.	Un nome array composto esclusivamente da numeri può causare problemi con il server SMI-S. Prova a cambiare il nome dell'array.
L'utente SMI-S configurato non ha alcun dominio	Concedi i privilegi di dominio appropriati all'utente SMI-S configurato
Data Infrastructure Insights afferma di non riuscire a connettersi/accedere al servizio SMI-S.	Verificare che non vi sia alcun firewall tra la CI AU e l'array che impedisca alla CI AU di effettuare connessioni TCP a 5988 o 5989. Una volta fatto ciò, e se hai confermato che non c'è alcun firewall, dovresti connetterti tramite SSH all'array e usare il comando "showcim" per confermare. Verificare che: * Il servizio sia abilitato * HTTPS sia abilitato * La porta HTTPS sia 5989 Se tutti questi punti sono corretti, è possibile provare a eseguire "stopcim" e quindi "startcim" per riavviare il CIM (ad esempio il servizio SMI-S).

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati HP Enterprise Command View

Il raccoglitore dati HP Enterprise Command View Advanced Edition supporta l'individuazione di array XP e P9500 tramite il server Command View Advanced Edition (CVAE). Data Infrastructure Insights comunica con CVAE tramite l'API standard Command View per raccogliere dati di inventario e prestazioni.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati HP Enterprise Command View. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
PDEV	Disco
Raccolta di riviste	Gruppo di dischi
Array di archiviazione	Magazzinaggio
Controllore di porta	Nodo di archiviazione
Gruppo di array, pool DP	Pool di archiviazione
Unità logica, LDEV	Volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti di inventario

Per raccogliere i dati di inventario è necessario disporre di quanto segue:

- Indirizzo IP del server CVAE
- Nome utente e password di sola lettura per il software CVAE e privilegi peer
- Requisito portuale: 2001

Requisiti di prestazione

Per raccogliere dati sulle prestazioni è necessario soddisfare i seguenti requisiti:

- Prestazioni HDS USP, USP V e VSP
  - Performance Monitor deve essere dotato di licenza.
  - L'interruttore di monitoraggio deve essere abilitato.
  - Lo strumento di esportazione (Export.exe) deve essere copiato in Data Infrastructure Insights AU ed estratto in una posizione. Nelle AU Linux CI, assicurarsi che "cisys" abbia i permessi di lettura ed esecuzione.
  - La versione dello strumento di esportazione deve corrispondere alla versione del microcodice dell'array di destinazione.
- Prestazioni AMS:
  - Performance Monitor deve essere dotato di licenza.
  - L'utilità Storage Navigator Modular 2 (SNM2) CLI deve essere installata su Data Infrastructure Insights AU.
- Requisiti di rete
  - Gli strumenti di esportazione sono basati su Java e utilizzano RMI per comunicare con l'array. Questi strumenti potrebbero non essere compatibili con i firewall, in quanto potrebbero negoziare dinamicamente le porte TCP di origine e di destinazione a ogni invocazione. Inoltre, gli strumenti di esportazione di array di modelli diversi potrebbero comportarsi in modo diverso sulla rete: consultare HPE per i requisiti del modello.

Configurazione

Campo	Descrizione
Server di visualizzazione dei comandi	Indirizzo IP o nome di dominio completo del server Command View
Nome utente	Nome utente per il server Command View.
Password	Password utilizzata per il server Command View.
Dispositivi - Archiviazioni VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP	Elenco dispositivi per gli storage VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP. Ogni storage richiede: * IP dell'array: indirizzo IP dello storage * Nome utente: nome utente per lo storage * Password: password per lo storage * Cartella contenente i file JAR dell'utilità di esportazione

Campo	Descrizione
SNM2Devices - Archiviazione WMS/SMS/AMS	Elenco dispositivi per archivi WMS/SMS/AMS. Ogni storage richiede: * IP dell'array: indirizzo IP dello storage * Percorso CLI di Storage Navigator: percorso CLI SNM2 * Autenticazione account valida: selezionare per scegliere un'autenticazione account valida * Nome utente: nome utente per lo storage * Password: password per lo storage
Scegli Tuning Manager per le prestazioni	Ignora altre opzioni di prestazioni
Host del gestore di ottimizzazione	Indirizzo IP o nome di dominio completo del gestore di ottimizzazione
Porta del gestore di ottimizzazione	Porta utilizzata per Tuning Manager
Nome utente del responsabile della messa a punto	Nome utente per Tuning Manager
Password del gestore di ottimizzazione	Password per Tuning Manager

Nota: in HDS USP, USP V e VSP, qualsiasi disco può appartenere a più di un gruppo di array.

Configurazione avanzata

Campo	Descrizione
Porta del server di visualizzazione dei comandi	Porta utilizzata per Command View Server
HTTPS abilitato	Seleziona per abilitare HTTPS
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40.
Selezionare "Escludi" o "Includi" per specificare un elenco	Specificare se includere o escludere l'elenco di array sottostante durante la raccolta dei dati.
Escludi o includi dispositivi	Elenco separato da virgole di ID dispositivo o nomi di array da includere o escludere
Query Host Manager	Seleziona per interrogare il gestore host
Intervallo di polling delle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: l'utente non ha autorizzazioni sufficienti	Utilizzare un account utente diverso con maggiori privilegi o aumentare i privilegi dell'account utente configurato nel raccoglitore dati

Problema:	Prova questo:
Errore: l’elenco degli archivi è vuoto. O i dispositivi non sono configurati o l’utente non ha autorizzazioni sufficienti	* Utilizzare DeviceManager per verificare se i dispositivi sono configurati. * Utilizzare un account utente diverso con più privilegi o aumentare i privilegi dell’account utente
Errore: l’array di archiviazione HDS non è stato aggiornato per alcuni giorni	Scopri perché questa matrice non viene aggiornata in HP CommandView AE.

Prestazione

Problema:	Prova questo:
Errore: * Errore durante l’esecuzione dell’utilità di esportazione * Errore durante l’esecuzione del comando esterno	* Verificare che Export Utility sia installato sull’unità di acquisizione Data Infrastructure Insights * Verificare che la posizione di Export Utility sia corretta nella configurazione del data collector * Verificare che l’IP dell’array USP/R600 sia corretto nella configurazione del data collector * Verificare che il nome utente e la password siano corretti nella configurazione del data collector * Verificare che la versione di Export Utility sia compatibile con la versione del microcodice dell’array di archiviazione * Dall’unità di acquisizione Data Infrastructure Insights , aprire un prompt CMD ed effettuare le seguenti operazioni: - Cambiare la directory nella directory di installazione configurata - Provare a stabilire una connessione con l’array di archiviazione configurato eseguendo il file batch runWin.bat
Errore: accesso allo strumento di esportazione non riuscito per l’IP di destinazione	* Conferma che il nome utente/password siano corretti * Crea un ID utente principalmente per questo raccoglitore dati HDS * Conferma che nessun altro raccoglitore dati sia configurato per acquisire questo array
Errore: gli strumenti di esportazione hanno registrato "Impossibile ottenere l’intervallo di tempo per il monitoraggio".	* Verificare che il monitoraggio delle prestazioni sia abilitato sulla matrice. * Provare a richiamare gli strumenti di esportazione al di fuori di Data Infrastructure Insights per confermare che il problema si trova al di fuori di Data Infrastructure Insights.
Errore: * Errore di configurazione: Storage Array non supportato da Export Utility * Errore di configurazione: Storage Array non supportato da Storage Navigator Modular CLI	* Configurare solo gli array di archiviazione supportati. * Utilizzare "Filtra elenco dispositivi" per escludere array di archiviazione non supportati.
Errore: * Errore durante l’esecuzione del comando esterno * Errore di configurazione: Array di archiviazione non segnalato da Inventory * Errore di configurazione: la cartella di esportazione non contiene file jar	* Controllare la posizione dell’utilità di esportazione. * Verificare se l’array di archiviazione in questione è configurato nel server Command View. * Impostare l’intervallo di polling delle prestazioni come multiplo di 60 secondi.

Problema:	Prova questo:
Errore: * Errore Storage Navigator CLI * Errore durante l'esecuzione del comando auperform * Errore durante l'esecuzione del comando esterno	* Verificare che Storage Navigator Modular CLI sia installato sull'unità di acquisizione Data Infrastructure Insights * Verificare che la posizione di Storage Navigator Modular CLI sia corretta nella configurazione del data collector * Verificare che l'IP dell'array WMS/SMS/SMS sia corretto nella configurazione del data collector * Verificare che la versione di Storage Navigator Modular CLI sia compatibile con la versione del microcodice dell'array di archiviazione configurato nel data collector * Dall'unità di acquisizione Data Infrastructure Insights , aprire un prompt CMD ed effettuare le seguenti operazioni: - Cambiare la directory nella directory di installazione configurata - Provare a stabilire una connessione con l'array di archiviazione configurato eseguendo il seguente comando "auunitref.exe"
Errore: Errore di configurazione: Array di archiviazione non segnalato dall'inventario	Verificare se l'array di archiviazione in questione è configurato nel server Command View
Errore: * Nessun array registrato con Storage Navigator Modular 2 CLI * Array non registrato con Storage Navigator Modular 2 CLI * Errore di configurazione: Storage Array non registrato con StorageNavigator Modular CLI	* Aprire il prompt dei comandi e cambiare directory nel percorso configurato. * Eseguire il comando "set=STONAVM_HOME=." * Eseguire il comando "auunitref" * Verificare che l'output del comando contenga i dettagli dell'array con IP * Se l'output non contiene i dettagli dell'array, registrare l'array con Storage Navigator CLI: - Aprire il prompt dei comandi e cambiare directory nel percorso configurato - Eseguire il comando "set=STONAVM_HOME=." - Eseguire il comando "auunitaddauto -ip ${ip}". Sostituisci ${ip} con l'IP reale

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati HPE Alletra 6000

Il raccoglitore dati HP Enterprise Alletra 6000 (in precedenza Nimble) supporta i dati di inventario e prestazioni per gli array di storage Alletra 6000.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Vettore	Magazzinaggio
Disco	Disco

Termine del fornitore/modello	Termine Data Infrastructure Insights
Volume	Volume
Piscina	Pool di archiviazione
Iniziatore	Alias host di archiviazione
Controllore	Nodo di archiviazione
Interfaccia Fibre Channel	Controllore

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per raccogliere dati di inventario e configurazione dall'array di archiviazione, è necessario disporre di quanto segue:

- L'array deve essere installato e configurato e raggiungibile dal client tramite il suo nome di dominio completo (FQDN) o l'indirizzo IP di gestione dell'array.
- L'array deve eseguire NimbleOS 2.3.x o versione successiva.
- È necessario disporre di un nome utente e di una password validi per l'array con almeno il ruolo di livello "Operatore". Il ruolo "Ospite" non ha accesso sufficiente per comprendere le configurazioni dell'iniziatore.
- La porta 5392 deve essere aperta sull'array.

Per raccogliere dati sulle prestazioni dall'array di archiviazione è necessario disporre di quanto segue:

- L'array deve eseguire NimbleOS 4.0.0 o versione successiva
- L'array deve avere volumi configurati. L'unica API di prestazioni di NimbleOS è per i volumi e tutte le statistiche dei report di Data Infrastructure Insights derivano dalle statistiche sui volumi

Configurazione

Campo	Descrizione
Indirizzo IP di gestione dell'array	Nome di dominio completo (FQDN) o indirizzo IP di gestione dell'array.
Nome utente	Nome utente per l'array
Password	Password per l'array

Configurazione avanzata

Campo	Descrizione
Porta	Porta utilizzata da Nimble REST API. Il valore predefinito è 5392.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.

Nota: l'intervallo di polling delle prestazioni predefinito è di 300 secondi e non può essere modificato. Questo è l'unico intervallo supportato da HPE Alletra 6000.

Sistemi di dati Hitachi

Raccoglitore dati Hitachi Vantara Command Suite

Il raccoglitore dati Hitachi Vantara Command Suite supporta il server HiCommand Device Manager. Data Infrastructure Insights comunica con il server HiCommand Device Manager tramite l'API HiCommand standard.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Hitachi Vantara Command Suite. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
PDEV	Disco
Raccolta di riviste	Gruppo di dischi
Array di archiviazione	Magazzinaggio
Controllore di porta	Nodo di archiviazione
Gruppo di array, pool HDS	Pool di archiviazione
Unità logica, LDEV	Volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Magazzinaggio

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle landing page delle risorse di archiviazione HDS. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

- Nome: proviene direttamente dall'attributo "nome" di HDS HiCommand Device Manager tramite la chiamata API XML GetStorageArray
- Modello: proviene direttamente dall'attributo "arrayType" di HDS HiCommand Device Manager tramite la chiamata API XML GetStorageArray
- Fornitore – HDS
- Famiglia: proviene direttamente dall'attributo "arrayFamily" di HDS HiCommand Device Manager tramite la chiamata API XML GetStorageArray
- IP: questo è l'indirizzo IP di gestione dell'array, non un elenco esaustivo di tutti gli indirizzi IP sull'array
- Capacità grezza: valore base2 che rappresenta la somma della capacità totale di tutti i dischi in questo sistema, indipendentemente dal ruolo del disco.

Pool di archiviazione

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle pagine di destinazione delle risorse del pool di archiviazione HDS. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

- Tipo: Il valore qui sarà uno dei seguenti:
  - RISERVATO – se questo pool è dedicato a scopi diversi dai volumi di dati, ad esempio journaling, snapshot
  - Thin Provisioning: se si tratta di un pool HDP
  - Gruppo Raid: probabilmente non li vedrai per alcuni motivi:

    Data Infrastructure Insights adotta una posizione ferma per evitare a tutti i costi il doppio conteggio della capacità. Su HDS, in genere è necessario creare gruppi Raid da dischi, creare volumi pool su tali gruppi Raid e costruire pool (spesso HDP, ma potrebbero essere per scopi speciali) da tali volumi pool. Se Data Infrastructure Insights segnalasse sia i gruppi Raid sottostanti così come sono, sia i pool, la somma della loro capacità grezza supererebbe di gran lunga la somma dei dischi.

  Al contrario, il raccoglitore dati HDS Command Suite di Data Infrastructure Insights riduce arbitrariamente le dimensioni dei gruppi Raid in base alla capacità dei volumi del pool. Ciò potrebbe comportare che Data Infrastructure Insights non segnali affatto il gruppo Raid. Inoltre, tutti i gruppi Raid risultanti vengono contrassegnati in modo tale da non essere visibili nella WebUI Data Infrastructure Insights , ma confluiscono nel Data Warehouse (DWH) di Data Data Infrastructure Insights . Lo scopo di queste decisioni è quello di evitare di sovraccaricare l'interfaccia utente con elementi che non interessano alla maggior parte degli utenti: se il tuo array HDS ha gruppi Raid con 50 MB liberi, probabilmente non potrai utilizzare quello spazio libero per alcun risultato significativo.

- Nodo - N/D, poiché i pool HDS non sono vincolati a nessun nodo specifico
- Ridondanza: il livello RAID del pool. Possibili valori multipli per un pool HDP composto da più tipi RAID
- Capacità %: la percentuale utilizzata del pool per l'utilizzo dei dati, con i GB utilizzati e la dimensione totale in GB logici del pool
- Capacità sovraimpegnata: un valore derivato che indica che "la capacità logica di questo pool è sovrascritta di questa percentuale in virtù della somma dei volumi logici che superano la capacità logica del pool di questa percentuale"
- Snapshot: mostra la capacità riservata per l'utilizzo degli snapshot su questo pool

Nodo di archiviazione

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle pagine di destinazione delle risorse dei nodi di archiviazione HDS. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

- Nome: il nome del Front-end Director (FED) o del Channel Adapter su array monolitici, oppure il nome del controller su un array modulare. Un dato array HDS avrà 2 o più nodi di archiviazione
- Volumi: la tabella Volume mostrerà qualsiasi volume mappato a qualsiasi porta di proprietà di questo nodo di archiviazione

Requisiti di inventario

Per raccogliere i dati di inventario è necessario disporre di quanto segue:

- Indirizzo IP del server HiCommand Device Manager
- Nome utente e password di sola lettura per il software HiCommand Device Manager e privilegi peer
- Requisiti porta: 2001 (http) o 2443 (https)
- Accedi al software HiCommand Device Manager utilizzando nome utente e password

- Verificare l’accesso a HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

Requisiti di prestazione

Per raccogliere dati sulle prestazioni è necessario soddisfare i seguenti requisiti:

- Prestazioni HDS USP, USP V e VSP
  - Performance Monitor deve essere dotato di licenza.
  - L’interruttore di monitoraggio deve essere abilitato.
  - Lo strumento di esportazione (Export.exe) deve essere copiato in Data Infrastructure Insights AU.
  - La versione dello strumento di esportazione deve corrispondere alla versione del microcodice dell’array di destinazione.
- Prestazioni AMS:
  - NetApp consiglia vivamente di creare un account di servizio dedicato sugli array AMS affinché Data Infrastructure Insights possa utilizzarlo per recuperare i dati sulle prestazioni. Storage Navigator consente a un account utente un solo accesso simultaneo all’array. Se Data Infrastructure Insights utilizza lo stesso account utente degli script di gestione o di HiCommand , Data Infrastructure Insights, gli script di gestione o HiCommand potrebbero non essere in grado di comunicare con l’array a causa del limite di un account utente contemporaneamente.
  - Performance Monitor deve essere dotato di licenza.
  - L’utilità Storage Navigator Modular 2 (SNM2) CLI deve essere installata su Data Infrastructure Insights AU.

Configurazione

Campo	Descrizione
Server HiCommand	Indirizzo IP o nome di dominio completo del server HiCommand Device Manager
Nome utente	Nome utente per il server HiCommand Device Manager.
Password	Password utilizzata per il server HiCommand Device Manager.
Dispositivi - Archiviazioni VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP	Elenco dispositivi per gli storage VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP. Ogni storage richiede: * IP dell’array: indirizzo IP dello storage * Nome utente: nome utente per lo storage * Password: password per lo storage * Cartella contenente i file JAR dell’utilità di esportazione
SNM2Devices - Archiviazione WMS/SMS/AMS	Elenco dispositivi per archivi WMS/SMS/AMS. Ogni storage richiede: * IP dell’array: indirizzo IP dello storage * Percorso CLI di Storage Navigator: percorso CLI SNM2 * Autenticazione account valida: selezionare per scegliere un’autenticazione account valida * Nome utente: nome utente per lo storage * Password: password per lo storage
Scegli Tuning Manager per le prestazioni	Ignora altre opzioni di prestazioni

Campo	Descrizione
Host del gestore di ottimizzazione	Indirizzo IP o nome di dominio completo del gestore di ottimizzazione
Sostituisci la porta del gestore di ottimizzazione	Se vuoto, utilizzare la porta predefinita nel campo Scegli Tuning Manager per le prestazioni, altrimenti immettere la porta da utilizzare
Nome utente del responsabile della messa a punto	Nome utente per Tuning Manager
Password del gestore di ottimizzazione	Password per Tuning Manager

Nota: in HDS USP, USP V e VSP, qualsiasi disco può appartenere a più di un gruppo di array.

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS o HTTP, visualizza anche la porta predefinita
Porta del server HiCommand	Porta utilizzata per HiCommand Device Manager
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40.
Selezionare "Escludi" o "Includi" per specificare un elenco	Specificare se includere o escludere l'elenco di array sottostante durante la raccolta dei dati.
Elenco dispositivi filtro	Elenco separato da virgole dei numeri di serie dei dispositivi da includere o escludere
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300.
Timeout di esportazione in secondi	Timeout dell'utilità di esportazione. Il valore predefinito è 300.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: l'utente non ha autorizzazioni sufficienti	Utilizzare un account utente diverso con maggiori privilegi o aumentare i privilegi dell'account utente configurato nel raccoglitore dati
Errore: l'elenco degli archivi è vuoto. O i dispositivi non sono configurati o l'utente non ha autorizzazioni sufficienti	* Utilizzare DeviceManager per verificare se i dispositivi sono configurati. * Utilizzare un account utente diverso con più privilegi o aumentare i privilegi dell'account utente
Errore: l'array di archiviazione HDS non è stato aggiornato per alcuni giorni	Scopri perché questo array non viene aggiornato in HDS HiCommand.

Prestazione

Problema:	Prova questo:
Errore: * Errore durante l'esecuzione dell'utilità di esportazione * Errore durante l'esecuzione del comando esterno	* Verificare che Export Utility sia installato sull'unità di acquisizione Data Infrastructure Insights * Verificare che la posizione di Export Utility sia corretta nella configurazione del data collector * Verificare che l'IP dell'array USP/R600 sia corretto nella configurazione del data collector * Verificare che il nome utente e la password siano corretti nella configurazione del data collector * Verificare che la versione di Export Utility sia compatibile con la versione del microcodice dell'array di archiviazione * Dall'unità di acquisizione Data Infrastructure Insights , aprire un prompt CMD ed effettuare le seguenti operazioni: - Cambiare la directory nella directory di installazione configurata - Provare a stabilire una connessione con l'array di archiviazione configurato eseguendo il file batch runWin.bat
Errore: accesso allo strumento di esportazione non riuscito per l'IP di destinazione	* Conferma che il nome utente/password siano corretti * Crea un ID utente principalmente per questo raccoglitore dati HDS * Conferma che nessun altro raccoglitore dati sia configurato per acquisire questo array
Errore: gli strumenti di esportazione hanno registrato "Impossibile ottenere l'intervallo di tempo per il monitoraggio".	* Verificare che il monitoraggio delle prestazioni sia abilitato sulla matrice. * Provare a richiamare gli strumenti di esportazione al di fuori di Data Infrastructure Insights per confermare che il problema si trova al di fuori di Data Infrastructure Insights.
Errore: * Errore di configurazione: Storage Array non supportato da Export Utility * Errore di configurazione: Storage Array non supportato da Storage Navigator Modular CLI	* Configurare solo gli array di archiviazione supportati. * Utilizzare "Filtra elenco dispositivi" per escludere array di archiviazione non supportati.
Errore: * Errore durante l'esecuzione del comando esterno * Errore di configurazione: Array di archiviazione non segnalato da Inventory * Errore di configurazione: la cartella di esportazione non contiene file jar	* Controllare la posizione dell'utilità di esportazione. * Verificare se l'array di archiviazione in questione è configurato nel server HiCommand. * Impostare l'intervallo di polling delle prestazioni come multiplo di 60 secondi.

Problema:	Prova questo:
Errore: * Errore Storage Navigator CLI * Errore durante l'esecuzione del comando auperform * Errore durante l'esecuzione del comando esterno	* Verificare che Storage Navigator Modular CLI sia installato sull'unità di acquisizione Data Infrastructure Insights * Verificare che la posizione di Storage Navigator Modular CLI sia corretta nella configurazione del data collector * Verificare che l'IP dell'array WMS/SMS/SMS sia corretto nella configurazione del data collector * Verificare che la versione di Storage Navigator Modular CLI sia compatibile con la versione del microcodice dell'array di archiviazione configurato nel data collector * Dall'unità di acquisizione Data Infrastructure Insights , aprire un prompt CMD ed effettuare le seguenti operazioni: - Cambiare la directory nella directory di installazione configurata - Provare a stabilire una connessione con l'array di archiviazione configurato eseguendo il seguente comando "auunitref.exe"
Errore: Errore di configurazione: Array di archiviazione non segnalato dall'inventario	Verificare se l'array di archiviazione in questione è configurato nel server HiCommand
Errore: * Nessun array registrato con Storage Navigator Modular 2 CLI * Array non registrato con Storage Navigator Modular 2 CLI * Errore di configurazione: Storage Array non registrato con StorageNavigator Modular CLI	* Aprire il prompt dei comandi e cambiare directory nel percorso configurato. * Eseguire il comando "set=STONAVM_HOME=." * Eseguire il comando "auunitref" * Verificare che l'output del comando contenga i dettagli dell'array con IP * Se l'output non contiene i dettagli dell'array, registrare l'array con Storage Navigator CLI: - Aprire il prompt dei comandi e cambiare directory nel percorso configurato - Eseguire il comando "set=STONAVM_HOME=." - Eseguire il comando "auunitaddauto -ip <ip>". Sostituisci <ip> con l'IP corretto.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati NAS Hitachi Vantara

Il raccoglitore dati Hitachi Vantara NAS è un raccoglitore dati di inventario e configurazione che supporta l'individuazione dei cluster NAS HDS. Data Infrastructure Insights supporta l'individuazione di condivisioni NFS e CIFS, file system (volumi interni) e span (pool di archiviazione).

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati HNAS. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Livello	Gruppo di dischi

Termine del fornitore/modello	Termine Data Infrastructure Insights
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
Span	Pool di archiviazione
Unità di sistema	Backend Lun
Sistema di file	Volume interno

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Indirizzo IP del dispositivo
- Porta 22, protocollo SSH
- Nome utente e password - livello di privilegio: Supervisore
- Nota: questo raccoglitore di dati è basato su SSH, quindi l'AU che lo ospita deve essere in grado di avviare sessioni SSH su TCP 22 sull'HNAS stesso o sulla Systems Management Unit (SMU) a cui è connesso il cluster.

Configurazione

Campo	Descrizione
Ospite HNAS	Indirizzo IP o nome di dominio completo dell'host di gestione HNAS
Nome utente	Nome utente per HNAS CLI
Password	Password utilizzata per HNAS CLI

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 30 minuti.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
"Errore di connessione" con messaggi di errore "Errore durante la configurazione del canale shell:" o "Errore durante l'apertura del canale shell"	Probabilmente causato da problemi di connettività di rete o da una configurazione errata di SSH. Conferma la connessione con il client SSH alternativo
"Timeout" o "Errore nel recupero dei dati" con messaggi di errore "Comando: XXX è scaduto."	* Prova il comando con un client SSH alternativo * Aumenta il timeout

Problema:	Prova questo:
"Errore di connessione" o "Credenziali di accesso non valide" con messaggi di errore "Impossibile comunicare con il dispositivo:"	* Controlla l'indirizzo IP * Controlla il nome utente e la password * Conferma la connessione con un client SSH alternativo

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Hitachi Ops Center

Questo raccoglitore di dati utilizza la suite integrata di applicazioni di Hitachi Ops Center per accedere ai dati di inventario e alle prestazioni di più dispositivi di archiviazione. Per l'individuazione dell'inventario e della capacità, l'installazione di Ops Center deve includere sia i componenti "Common Services" sia "Administrator". Per la raccolta delle prestazioni, è necessario che sia distribuito anche "Analyzer".

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore di dati. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Sistemi di archiviazione	Magazzinaggio
Volume	Volume
Gruppi di parità	Pool di archiviazione (RAID), gruppi di dischi
Disco	Disco
Pool di archiviazione	Pool di archiviazione (sottile, SNAP)
Gruppi di parità esterni	Pool di archiviazione (backend), gruppi di dischi
Porta	Nodo di archiviazione → Nodo controller → Porta
Gruppi ospitanti	Mappatura e mascheramento del volume
Coppie di volumi	Sincronizzazione dell'archiviazione

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti di inventario

Per raccogliere i dati di inventario è necessario disporre di quanto segue:

- Indirizzo IP o nome host del server Ops Center che ospita il componente "Common Services"
- Account utente root/sysadmin e password presenti su tutti i server che ospitano i componenti di Ops Center. HDS non ha implementato il supporto REST API per l'utilizzo da parte di utenti LDAP/SSO fino a Ops Center 10.8+

Requisiti di prestazione

Per raccogliere dati sulle prestazioni è necessario soddisfare i seguenti requisiti:

Il modulo "Analyzer" di HDS Ops Center deve essere installato. Gli array di storage devono alimentare il modulo "Analyzer" di Ops Center.

Configurazione

Campo	Descrizione
Indirizzo IP del centro operativo Hitachi	Indirizzo IP o nome di dominio completo del server Ops Center che ospita il componente "Common Services"
Nome utente	Nome utente per il server Ops Center.
Password	Password utilizzata per il server Ops Center.

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS (porta 443) è l'impostazione predefinita
Sostituisci porta TCP	Specificare la porta da utilizzare se non è quella predefinita
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40.
Selezionare "Escludi" o "Includi" per specificare un elenco	Specificare se includere o escludere l'elenco di array sottostante durante la raccolta dei dati.
Elenco dispositivi filtro	Elenco separato da virgole dei numeri di serie dei dispositivi da includere o escludere
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Infinidat InfiniBox

Il raccoglitore dati Infinidat InfiniBox (HTTP) viene utilizzato per raccogliere informazioni di inventario dal sistema di archiviazione Infinidat InfiniBox.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Infinidat InfiniBox. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Pool di archiviazione	Pool di archiviazione
Nodo	Controllore
File system	Volume interno
File system	Condivisione file
Esportazioni del file system	Condividere

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questo raccoglitore dati.

- Indirizzo IP o FQDN del nodo di gestione InfiniBox
- ID utente e password amministratore
- Porta 443 tramite API REST

Configurazione

Campo	Descrizione
Host InfiniBox	Indirizzo IP o nome di dominio completo del nodo di gestione InfiniBox
Nome utente	Nome utente per il nodo di gestione InfiniBox
Password	Password per il nodo di gestione InfiniBox

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per connettersi al server InfiniBox. Il valore predefinito è 443.
Intervallo di sondaggio dell'inventario	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Huawei OceanStor

Data Infrastructure Insights utilizza il raccoglitore di dati Huawei OceanStor (REST/HTTPS) per scoprire l'inventario e le prestazioni per lo storage Huawei OceanStor e OceanStor Dorado.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni sull'inventario e sulle prestazioni da Huawei OceanStor. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Pool di archiviazione	Pool di archiviazione
Sistema di file	Volume interno
Controllore	Nodo di archiviazione
Porta FC (Mappata)	Mappa del volume
Iniziatore FC host (mappato)	Maschera del volume
Condivisione NFS/CIFS	Condividere
Destinazione collegamento iSCSI	Nodo di destinazione iSCSI
Iniziatore di collegamento iSCSI	Nodo iniziatore iSCSI
Disco	Disco
LUN	Volume

Requisiti

Per configurare questo raccoglitore dati sono richiesti i seguenti requisiti:

- Indirizzo IP del dispositivo
- Credenziali per accedere al gestore dispositivi OceanStor
- La porta 8088 deve essere disponibile

Configurazione

Campo	Descrizione
Indirizzo IP host OceanStor	Indirizzo IP o nome di dominio completo di OceanStor Device Manager
Nome utente	Nome utilizzato per accedere a OceanStor Device Manager
Password	Password utilizzata per accedere a OceanStor Device Manager

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per connettersi a OceanStor Device Manager. Il valore predefinito è 8088.

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.
Intervallo di sondaggio delle prestazioni (sec).	Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

IBM

Raccoglitore dati IBM Cleversafe

Data Infrastructure Insights utilizza questo strumento di raccolta dati per scoprire dati di inventario e prestazioni per i sistemi di storage IBM Cleversafe.

IBM Cleversafe viene misurato in base a una tariffa Raw TB diversa da quella delle unità gestite. Ogni 40 TB di capacità IBM Cleversafe non formattata viene addebitato come 1"Unità gestita (MU)" .

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati IBM Cleversafe. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Pool di archiviazione	Pool di archiviazione
Contenitore	Volume interno
Contenitore	Condivisione file
Condivisione NFS	Condividere

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- L'indirizzo IP dei servizi dati esterni per il cluster
- Nome utente e password dell'amministratore
- Porta 9440

Configurazione

Campo	Descrizione
IP del gestore o nome host	Indirizzo IP o nome host del nodo di gestione

Campo	Descrizione
Nome utente	Nome utente per l'account utente con ruolo di superutente o amministratore di sistema
Password	Password per l'account utente con ruolo di superutente o amministratore di sistema

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario.
Timeout della connessione HTTP (sec)	Timeout HTTP in secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati IBM CS

Data Infrastructure Insights utilizza questo strumento di raccolta dati per scoprire dati di inventario e prestazioni per i sistemi di storage IBM CS.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati IBM CS. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Pool di archiviazione	Pool di archiviazione
Contenitore	Volume interno
Contenitore	Condivisione file
Condivisione NFS	Condividere

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- L'indirizzo IP dei servizi dati esterni per il cluster
- Nome utente e password dell'amministratore
- Porta 9440

Configurazione

Campo	Descrizione
Indirizzo IP esterno Prism	L'indirizzo IP dei servizi dati esterni per il cluster
Nome utente	Nome utente per l'account amministratore
Password	Password per l'account amministratore

Configurazione avanzata

Campo	Descrizione
porta TCP	Porta TCP utilizzata per connettersi all'array IBM CS. Il valore predefinito è 9440.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.
Intervallo di sondaggio delle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati IBM System Storage serie DS8000

Il raccoglitore dati IBM DS (CLI) supporta l'acquisizione di dati di inventario e prestazioni per i dispositivi DS6xxx e DS8xxx.

I dispositivi DS3xxx, DS4xxx e DS5xxx sono supportati da"Raccoglitore dati NetApp E-Series" . Per i modelli supportati e le versioni del firmware, fare riferimento alla matrice di supporto Data Infrastructure Insights .

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati IBM DS. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Modulo unità disco	Disco
Immagine di archiviazione	Magazzinaggio
Pool di estensione	Nodo di archiviazione
Volume di blocco fisso	Volume
Iniziatore FC host (mappato)	Maschera del volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati è necessario quanto segue:

- Indirizzo IP di ogni array DS
- Nome utente e password di sola lettura su ogni array DS
- Software di terze parti installato su Data Infrastructure Insights AU: IBM *dscli*
- Validazione dell'accesso: eseguire i comandi *dscli* utilizzando il nome utente e la password
- Requisiti delle porte: 80, 443 e 1750

Configurazione

Campo	Descrizione
Archiviazione DS	Indirizzo IP o nome di dominio completo del dispositivo DS
Nome utente	Nome utente per DS CLI
Password	Password per la CLI DS
percorso eseguibile *dscli*	Percorso completo dell'eseguibile *dscli*

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario (min). Il valore predefinito è 40.
Nome visualizzato di archiviazione	Nome dell'array di archiviazione IBM DS
Dispositivi esclusi dall'inventario	Elenco separato da virgole dei numeri di serie dei dispositivi da escludere dalla raccolta dell'inventario
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 300.
Tipo di filtro delle prestazioni	Includi: dati raccolti solo dai dispositivi presenti nell'elenco. Escludi: nessun dato da questi dispositivi viene raccolto
Elenco dispositivi filtro prestazioni	Elenco separato da virgole degli ID dispositivo da includere o escludere dalla raccolta delle prestazioni

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore contenente: CMUC00192E, CMUC00191E o CMUC00190E	* Verificare le credenziali e l'indirizzo IP immessi. * Provare a comunicare con l'array tramite la console di gestione Web https://<ip>:8452/DS8000/Console. Sostituisci <ip> con l'IP configurato dal raccoglitore dati.
Errore: * Impossibile eseguire il programma * Errore durante l'esecuzione del comando	* Da Data Infrastructure Insights Acquisition Unit, aprire un CMD * Aprire il file CLI.CFG nella directory/lib home della CLI e controllare la proprietà JAVA_INSTALL, modificare il valore in modo che corrisponda al proprio ambiente * Visualizzare la versione Java installata su questa macchina, digitando: "java -version" * Eseguire il ping dell'indirizzo IP del dispositivo IBM Storage specificato nel comando CLI emesso. * Se tutto quanto sopra ha funzionato correttamente, eseguire manualmente un comando CLI

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati IBM SAN Volume Controller

Il raccoglitore dati IBM SAN Volume Controller (SVC) raccoglie dati di inventario e prestazioni tramite SSH, supportando una varietà di dispositivi che eseguono il sistema operativo SVC.

L'elenco dei dispositivi supportati include modelli quali SVC, v7000, v5000 e v3700. Per i modelli supportati e le versioni del firmware, fare riferimento alla matrice di supporto Data Infrastructure Insights .

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati IBM SVC. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Guidare	Disco
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
Gruppo Mdisk	Pool di archiviazione
Vdisk	Volume
Mdisk	LUN e percorsi backend

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti di inventario

- Indirizzo IP di ciascun cluster SVC
- Porta 22 disponibile
- Nome utente e password di sola lettura

Requisiti di prestazione

- Console SVC, obbligatoria per qualsiasi cluster SVC e richiesta per il pacchetto SVC Discovery Foundation.
- Le credenziali richiederanno il livello di accesso amministrativo solo per copiare i file delle prestazioni dai nodi del cluster al nodo di configurazione.
- Abilita la raccolta dati connettendoti al cluster SVC tramite SSH ed eseguendo: *svctask startstats -interval 1*

  Nota: in alternativa, abilitare la raccolta dati tramite l'interfaccia utente di gestione SVC.

Configurazione

Campo	Descrizione
Indirizzi IP del cluster	Indirizzi IP o nomi di dominio completi dell'archiviazione SVC
Nome utente inventario	Nome utente per la CLI SVC
Password di inventario	Password per la CLI SVC

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti.
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.
Per ripulire i file delle statistiche scaricati	Seleziona questa casella di controllo per ripulire i file delle statistiche scaricate

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Problema:	Prova questo:
Errore: "Impossibile avviare il comando perché non è stato eseguito sul nodo di configurazione."	Il comando deve essere eseguito sul nodo di configurazione.

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Problema:	Prova questo:
Errore: "Impossibile avviare il comando perché non è stato eseguito sul nodo di configurazione."	Il comando deve essere eseguito sul nodo di configurazione.

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati IBM XIV/A9000

Il raccoglitore dati IBM XIV e A9000 (CLI) utilizza l'interfaccia della riga di comando XIV per raccogliere i dati di inventario, mentre la raccolta delle prestazioni viene eseguita effettuando chiamate SMI-S all'array XIV/A9000, che esegue un provider SMI-S sulla porta 7778.

Terminologia

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Sistema di archiviazione	Magazzinaggio
Pool di archiviazione	Pool di archiviazione
Volume	Volume

Requisiti

Per configurare e utilizzare questo raccoglitore dati è necessario soddisfare i seguenti requisiti:

- Requisito porta: porta TCP 7778
- Nome utente e password di sola lettura
- La CLI XIV deve essere installata sull'AU

Requisiti di prestazione

Di seguito sono riportati i requisiti per la riscossione delle prestazioni:

- SMI-S Agent 1.4 o superiore
- CIMService compatibile con SMI-S in esecuzione su array. La maggior parte degli array XIV ha un CIMServer installato di default.
- È necessario fornire l'accesso utente per CIMServer. L'accesso deve avere accesso completo in lettura alla configurazione e alle proprietà dell'array.
- Spazio dei nomi SMI-S. L'impostazione predefinita è root/ibm. Questa opzione è configurabile in CIMServer.
- Requisiti porta: 5988 per HTTP, 5989 per HTTPS.
- Per informazioni su come creare un account per la raccolta delle prestazioni SMI-S, fare riferimento al seguente collegamento: https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

Configurazione

Campo	Descrizione
XIV indirizzo IP	Indirizzo IP o nome di dominio completo dello storage XIV
Nome utente	Nome utente per l'archiviazione XIV
Password	Password per l'archiviazione XIV
Percorso completo alla directory XIV CLI	Percorso completo della cartella contenente la CLI XIV
Indirizzo IP host SMI-S	Indirizzo IP dell'host SMI-S

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti.
Protocollo SMI-S	Protocollo utilizzato per connettersi al provider SMI-S. Visualizza anche la porta predefinita.
Sostituisci porta SMI-S	Se vuoto, utilizzare la porta predefinita nel campo Tipo di connessione, altrimenti immettere la porta di connessione da utilizzare
Nome utente	Nome utente per l'host del provider SMI-S
Password	Password per l'host del provider SMI-S
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Lenovo

Data Infrastructure Insights utilizza il raccoglitore dati Lenovo per scoprire dati di inventario e prestazioni per i sistemi di storage Lenovo HX.

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Indirizzo IP esterno Prism
- Nome utente e password dell'amministratore
- Porta TCP richiesta: 9440

Configurazione

Campo	Descrizione
Indirizzo IP esterno Prism	L'indirizzo IP dei servizi dati esterni per il cluster
Nome utente	Nome utente per l'account amministratore
Password	Password per l'account amministratore

Configurazione avanzata

Campo	Descrizione
porta TCP	Porta TCP utilizzata per connettersi all'array. Il valore predefinito è 9440.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.
Intervallo di sondaggio delle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Microsoft

Configurazione del raccoglitore dati Azure NetApp Files

Data Infrastructure Insights utilizza il raccoglitore dati Azure NetApp Files per acquisire dati di inventario e prestazioni.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni.

- Requisito porta: 443 HTTPS
- IP REST di gestione di Azure (management.azure.com)
- ID client dell'entità servizio di Azure (account utente)
- Chiave di autenticazione dell'entità servizio di Azure (password utente)
- È necessario configurare un account Azure per l'individuazione di Data Infrastructure Insights .

  Una volta configurato correttamente l'account e registrata l'applicazione in Azure, si avranno le credenziali necessarie per individuare l'istanza di Azure con Data Infrastructure Insights. Il seguente link descrive come impostare l'account per la scoperta:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configurazione

Inserire i dati nei campi del raccoglitore dati secondo la tabella seguente:

Campo	Descrizione
ID client dell'entità servizio di Azure	ID di accesso ad Azure
ID tenant di Azure	ID tenant di Azure
Chiave di autenticazione dell'entità servizio di Azure	Chiave di autenticazione di accesso
Capisco che Microsoft mi fattura le richieste API	Seleziona questa casella per verificare di aver compreso che Microsoft ti addebita le richieste API effettuate tramite polling di Insight.

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60

Risoluzione dei problemi

- Le credenziali utilizzate dal raccoglitore dati ANF devono avere accesso a tutte le sottoscrizioni di Azure che contengono volumi ANF.
- Se l'accesso come lettore causa il fallimento della raccolta delle prestazioni, provare a concedere l'accesso come collaboratore a livello di gruppo di risorse.

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Microsoft Hyper-V

Il raccoglitore dati Microsoft Hyper-V acquisisce dati di inventario e prestazioni dall'ambiente di elaborazione del server virtualizzato. Questo raccoglitore di dati può rilevare un host Hyper-V autonomo o un intero cluster: creare un raccoglitore per ogni host autonomo o cluster.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da Microsoft Hyper-V (WMI). Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco rigido virtuale	Disco virtuale
Ospite	Ospite
Macchina virtuale	Macchina virtuale
Cluster Shared Volumes (CSV), Volume di partizione	Archivio dati

Termine del fornitore/modello	Termine Data Infrastructure Insights
Dispositivo SCSI Internet, LUN SCSI multipercorso	LUN
Porta Fibre Channel	Porta

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessari i seguenti elementi:

- Hyper-V richiede l'apertura della porta 5985 per la raccolta dati e l'accesso/gestione remota.
- Indirizzo IP o FQDN del cluster o dell'hypervisor autonomo. Utilizzare il nome host o l'IP del cluster mobile è probabilmente l'approccio più affidabile rispetto all'indirizzare il collettore a un solo nodo specifico in un cluster.
- Account utente di livello amministrativo che funziona su tutti gli hypervisor del cluster.
- WinRM deve essere abilitato e in ascolto su tutti gli hypervisor
- Requisiti delle porte: porta 135 tramite WMI e porte TCP dinamiche assegnate 1024-65535 per Windows 2003 e versioni precedenti e 49152-65535 per Windows 2008.
- La risoluzione DNS deve riuscire, anche se il raccoglitore dati è puntato solo a un indirizzo IP
- Ogni hypervisor Hyper-V deve avere la funzione "Resource Metering" attivata per ogni VM, su ogni host. Ciò consente a ciascun hypervisor di avere a disposizione più dati per Data Infrastructure Insights su ciascun guest. Se questa opzione non viene impostata, per ogni ospite vengono acquisite meno metriche sulle prestazioni. Ulteriori informazioni sulla misurazione delle risorse sono disponibili nella documentazione Microsoft:

  "Panoramica sulla misurazione delle risorse di Hyper-V"

  "Abilita-VMResourceMetering"

Il raccoglitore dati Hyper-V richiede una Windows Acquisition Unit.

Configurazione

Campo	Descrizione
Indirizzo IP del cluster o FQDN del cluster mobile	L'indirizzo IP o il nome di dominio completo per il cluster o un hypervisor autonomo e non in cluster
Nome utente	Nome utente amministratore per l'hypervisor
Password	Password per l'hypervisor
Suffisso di dominio DNS	Il suffisso del nome host che si combina con il nome host semplice per rendere l'FQDN di un hypervisor

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 20 minuti.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

NetApp

Raccoglitore dati NetApp Cloud Volumes ONTAP

Questo raccoglitore dati supporta la raccolta di inventario dalle configurazioni Cloud Volumes ONTAP .

Configurazione

Campo	Descrizione
Indirizzo IP di gestione NetApp	Indirizzo IP per Cloud Volumens ONTAP
Nome utente	Nome utente per Cloud Volumes ONTAP
Password	Password per l'utente sopra indicato

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	Si consiglia HTTPS. Mostra anche la porta predefinita.
Sostituisci porta di comunicazione	Porta da utilizzare se non è quella predefinita.
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti.
Conteggio dei thread simultanei dell'inventario	Numero di thread simultanei.
Forza TLS per HTTPS	Forza TLS su HTTPS
Ricerca automatica dei netgroup	Ricerca automatica dei netgroup
Espansione di Netgroup	Seleziona Shell o File
Timeout di lettura HTTP in secondi	Il valore predefinito è 30 secondi
Forza le risposte come UTF-8	Forza le risposte come UTF-8
Intervallo di sondaggio sulle prestazioni (min)	Il valore predefinito è 900 secondi.
Numero di thread simultanei delle prestazioni	Numero di thread simultanei.
Raccolta dati avanzata del contatore	Selezionare questa opzione per consentire a Data Infrastructure Insights di raccogliere le metriche avanzate dall'elenco seguente.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati AFX NetApp ONTAP

Questo raccoglitore di dati acquisisce dati di inventario, registri EMS e dati sulle prestazioni dai sistemi di archiviazione che eseguono ONTAP 9.16.0 e versioni successive utilizzando chiamate API REST.

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questo raccoglitore dati:

- È necessario avere accesso a un account utente con il livello di accesso richiesto. Si noti che sono necessarie le autorizzazioni di amministratore se si crea un nuovo utente/ruolo REST.
  - Dal punto di vista funzionale, Data Infrastructure Insights esegue principalmente richieste di lettura, ma sono necessarie alcune autorizzazioni di scrittura affinché Data Infrastructure Insights possa registrarsi con l'array ONTAP . Vedere la *Nota sulle autorizzazioni* subito sotto.
- ONTAP versione 9.16.0 o successiva.
- Requisiti della porta: 443

Una nota sui permessi

Poiché numerose dashboard ONTAP di Data Infrastructure Insights si basano su contatori ONTAP avanzati, è consigliabile mantenere abilitata l'opzione **Abilita raccolta dati contatore avanzata** nella sezione Configurazione avanzata del raccoglitore dati.

Per creare un account locale per Data Infrastructure Insights a livello di cluster, accedere a ONTAP con il nome utente/password dell'amministratore di gestione del cluster ed eseguire i seguenti comandi sul server ONTAP :

1. Prima di iniziare, è necessario aver effettuato l'accesso a ONTAP con un account *Amministratore* e i *comandi a livello diagnostico* devono essere abilitati.
2. Recupera il nome del vserver di tipo *admin*. Utilizzerai questo nome nei comandi successivi.

```
 vserver show -type admin
. Crea un ruolo utilizzando i seguenti comandi:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Creare l'utente di sola lettura utilizzando il seguente comando. Dopo aver eseguito il comando create, ti verrà chiesto di immettere una password per questo utente.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Se viene utilizzato un account AD/LDAP, il comando deve essere

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Il ruolo risultante e l'accesso utente saranno simili ai seguenti.  Il
risultato effettivo potrebbe variare:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                 Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migrazione

Per migrare da un precedente raccoglitore dati ONTAP (ontapi) al più recente raccoglitore REST ONTAP , procedere come segue:

1. Aggiungere il REST Collector. Si consiglia di immettere le informazioni per un utente diverso da quello configurato per il raccoglitore precedente. Ad esempio, utilizzare l'utente indicato nella sezione Autorizzazioni sopra.
2. Mette in pausa il raccoglitore precedente, in modo che non continui a raccogliere dati.
3. Lasciare che il nuovo collettore REST acquisisca i dati per almeno 30 minuti. Ignorare tutti i dati che durante questo periodo non sembrano "normali".

4. Dopo il periodo di riposo, dovresti vedere i tuoi dati stabilizzarsi mentre il collettore REST continua ad acquisire.

Se lo desideri, puoi usare lo stesso procedimento per tornare al collettore precedente.

Configurazione

Campo	Descrizione
Indirizzo IP di gestione ONTAP	Indirizzo IP o nome di dominio completo del cluster NetApp . Deve essere l'IP/FQDN di gestione del cluster.
Nome utente ONTAP REST	Nome utente per il cluster NetApp
Password ONTAP REST	Password per il cluster NetApp

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti.
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 60 secondi.
Raccolta dati avanzata del contatore	Selezionare questa opzione per includere i dati del contatore avanzato ONTAP nei sondaggi. Abilitato per impostazione predefinita.
Abilita raccolta eventi EMS	Selezionare questa opzione per includere i dati degli eventi del registro ONTAP EMS. Abilitato per impostazione predefinita.
Intervallo di interrogazione EMS (sec)	Il valore predefinito è 60 secondi.

Terminologia

Data Infrastructure Insights acquisisce dati di inventario, registri e prestazioni dal raccoglitore dati ONTAP . Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per l'asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Grappolo	Magazzinaggio
Nodo	StorageNode
Volume/ FlexVol/ FlexGroup	Volume interno
Qtree/FlexTree	Qtree (tipo: Esplixit/Default)
Secchio S3	Qtree (tipo: Bucket)
StoragePod/StorageAvailabilityZone	StoragePool
Condividere	Condividere
Quota	Quota

Termine del fornitore/modello	Termine Data Infrastructure Insights
SVM (macchina virtuale di archiviazione)	Macchina virtuale di archiviazione

Terminologia di gestione dei dati ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle pagine di destinazione delle risorse di archiviazione ONTAP Data Management. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

Magazzinaggio

- Modello: elenco delimitato da virgole dei nomi univoci e discreti dei modelli di nodi all'interno di questo cluster. Se tutti i nodi nei cluster sono dello stesso tipo di modello, verrà visualizzato un solo nome di modello.
- Fornitore: lo stesso nome del fornitore che vedresti se stessi configurando una nuova origine dati.
- Numero di serie: l'UUID dell'array
- IP: in genere saranno gli IP o i nomi host configurati nell'origine dati.
- Versione del microcodice – firmware.
- Capacità grezza: somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo.
- Latenza: rappresentazione di ciò che sta sperimentando l'host sottoposto a carichi di lavoro, sia in lettura che in scrittura. Idealmente, Data Infrastructure Insights reperirebbe questo valore direttamente, ma spesso non è così. Invece dell'array che offre questa funzionalità, Data Infrastructure Insights esegue in genere un calcolo ponderato in base agli IOPS derivato dalle statistiche dei singoli volumi interni.
- Capacità di elaborazione: aggregata dai volumi interni. Gestione: può contenere un collegamento ipertestuale all'interfaccia di gestione del dispositivo. Creato a livello di programmazione dalla fonte dati Data Infrastructure Insights come parte della reportistica di inventario.

Pool di archiviazione

- Archiviazione: su quale array di archiviazione risiede questo pool. Obbligatorio.
- Tipo: un valore descrittivo da un elenco di possibilità enumerate. Nella maggior parte dei casi sarà "Aggregato" o "Gruppo RAID".
- Nodo: se l'architettura di questo array di archiviazione è tale che i pool appartengono a un nodo di archiviazione specifico, il suo nome verrà visualizzato qui come collegamento ipertestuale alla relativa landing page.
- Utilizza Flash Pool – Valore Sì/No – questo pool basato su SATA/SAS ha SSD utilizzati per l'accelerazione della memorizzazione nella cache?
- Ridondanza: livello RAID o schema di protezione. RAID_DP è a doppia parità, RAID_TP è a tripla parità.
- Capacità: i valori qui indicati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata tra queste.
- Capacità sovraimpegnata: se utilizzando tecnologie di efficienza è stata assegnata una somma totale di volume o capacità di volume interno superiore alla capacità logica del pool di archiviazione, il valore percentuale sarà maggiore dello 0%.
- Snapshot: capacità di snapshot utilizzate e totali, se l'architettura del pool di archiviazione dedica parte della sua capacità ad aree di segmenti esclusivamente per gli snapshot. È probabile che le configurazioni ONTAP in MetroCluster presentino questo fenomeno, mentre altre configurazioni ONTAP lo presentano in misura minore.

- Utilizzo: valore percentuale che indica la percentuale più alta di disco occupato tra tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. L'utilizzo del disco non ha necessariamente una forte correlazione con le prestazioni dell'array: l'utilizzo può essere elevato a causa di ricostruzioni del disco, attività di deduplicazione, ecc. in assenza di carichi di lavoro gestiti dall'host. Inoltre, molte implementazioni di replicazione degli array possono aumentare l'utilizzo del disco senza essere visualizzate come volume interno o carico di lavoro del volume.
- IOPS: la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Throughput: la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione.

Nodo di archiviazione

- Archiviazione: di quale array di archiviazione fa parte questo nodo. Obbligatorio.
- Partner HA: sulle piattaforme in cui un nodo esegue il failover su un solo altro nodo, in genere verrà visualizzato qui.
- Stato: salute del nodo. Disponibile solo quando l'array è sufficientemente integro da poter essere inventariato da una fonte dati.
- Modello: nome del modello del nodo.
- Versione: nome della versione del dispositivo.
- Numero di serie: il numero di serie del nodo.
- Memoria: memoria base 2 se disponibile.
- Utilizzo: su ONTAP, si tratta di un indice di stress del controller derivante da un algoritmo proprietario. A ogni sondaggio sulle prestazioni verrà segnalato un numero compreso tra 0 e 100%, che rappresenta il valore più alto tra la contesa del disco WAFL o l'utilizzo medio della CPU. Se si osservano valori sostenuti > 50%, ciò è indicativo di sottodimensionamento, ovvero un controller/nodo non sufficientemente grande o un numero insufficiente di dischi rotanti per assorbire il carico di lavoro di scrittura.
- IOPS – Derivato direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Latenza: derivata direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Throughput: derivato direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Processori: numero di CPU.

Metriche di potenza ONTAP

Diversi modelli ONTAP forniscono metriche di potenza per Data Infrastructure Insights che possono essere utilizzate per il monitoraggio o l'invio di avvisi. Gli elenchi dei modelli supportati e non supportati riportati di seguito non sono esaustivi, ma dovrebbero fornire alcune indicazioni; in generale, se un modello appartiene alla stessa famiglia di uno presente nell'elenco, il supporto dovrebbe essere lo stesso.

Modelli supportati:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelli non supportati:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Problema:	Prova questo:
Quando si tenta di creare un raccoglitore di dati REST ONTAP , viene visualizzato un errore simile al seguente: Configurazione: 10.193.70.14: l'API REST ONTAP su 10.193.70.14 non è disponibile: 10.193.70.14 non è riuscito a GET /api/cluster: 400 Richiesta non valida	Ciò è probabilmente dovuto a un array ONTAP più vecchio (ad esempio ONTAP 9.6) che non ha funzionalità API REST. ONTAP 9.14.1 è la versione minima ONTAP supportata dal collettore REST ONTAP . Nelle versioni precedenti a REST ONTAP ci si dovrebbe aspettare risposte "400 Bad Request". Per le versioni ONTAP che supportano REST ma non sono 9.14.1 o successive, potrebbe essere visualizzato il seguente messaggio simile: Configurazione: 10.193.98.84: l'API REST ONTAP su 10.193.98.84 non è disponibile: 10.193.98.84: l'API REST ONTAP su 10.193.98.84 è disponibile: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ma non è della versione minima 9.14.1.
Vedo metriche vuote o "0" dove il collettore ONTAP ontapi mostra i dati.	ONTAP REST non segnala metriche utilizzate internamente solo sul sistema ONTAP . Ad esempio, gli aggregati di sistema non verranno raccolti da ONTAP REST, ma solo gli SVM di tipo "dati". Altri esempi di metriche ONTAP REST che potrebbero segnalare dati pari a zero o vuoti: InternalVolumes: REST non segnala più vol0. Aggregati: REST non segnala più aggr0. Archiviazione: la maggior parte delle metriche è un riepilogo delle metriche del volume interno e sarà influenzata da quanto sopra. Macchine virtuali di archiviazione: REST non segnala più SVM di tipo diverso da "dati" (ad esempio "cluster", "mgmt", "nodo"). Potresti anche notare un cambiamento nell'aspetto dei grafici che contengono dati, dovuto alla modifica del periodo di polling delle prestazioni predefinito da 15 a 5 minuti. Sondaggi più frequenti significano più punti dati da tracciare.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati NetApp ONTAP ASA r2 (All-SAN Array)

Questo raccoglitore di dati acquisisce dati di inventario, registri EMS e dati sulle prestazioni dai sistemi di archiviazione che eseguono ONTAP 9.16.0 e versioni successive utilizzando chiamate API REST.

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questo raccoglitore dati:

- È necessario avere accesso a un account utente con il livello di accesso richiesto. Si noti che sono necessarie le autorizzazioni di amministratore se si crea un nuovo utente/ruolo REST.

- Dal punto di vista funzionale, Data Infrastructure Insights esegue principalmente richieste di lettura, ma sono necessarie alcune autorizzazioni di scrittura affinché Data Infrastructure Insights possa registrarsi con l'array ONTAP . Vedere la *Nota sulle autorizzazioni* subito sotto.

- ONTAP versione 9.16.0 o successiva.
- Requisiti della porta: 443

ASA R2 indica i modelli di ultima generazione della piattaforma di storage ONTAP ASA . Sono inclusi i modelli array ASA A1K, A90, A70, A50, A30 e A20.

Per tutti i sistemi ASA di generazione precedente, utilizzare"ONTAP REST" collettore.

Una nota sui permessi

Poiché numerose dashboard ONTAP di Data Infrastructure Insights si basano su contatori ONTAP avanzati, è consigliabile mantenere abilitata l'opzione **Abilita raccolta dati contatore avanzata** nella sezione Configurazione avanzata del raccoglitore dati.

Per creare un account locale per Data Infrastructure Insights a livello di cluster, accedere a ONTAP con il nome utente/password dell'amministratore di gestione del cluster ed eseguire i seguenti comandi sul server ONTAP :

1. Prima di iniziare, è necessario aver effettuato l'accesso a ONTAP con un account *Amministratore* e i *comandi a livello diagnostico* devono essere abilitati.
2. Recupera il nome del vserver di tipo *admin*. Utilizzerai questo nome nei comandi successivi.

```
 vserver show -type admin
. Crea un ruolo utilizzando i seguenti comandi:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Creare l'utente di sola lettura utilizzando il seguente comando. Dopo aver eseguito il comando create, ti verrà chiesto di immettere una password per questo utente.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Se viene utilizzato un account AD/LDAP, il comando deve essere

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Il ruolo risultante e l'accesso utente saranno simili ai seguenti.  Il
risultato effettivo potrebbe variare:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migrazione

Per migrare da un precedente raccoglitore dati ONTAP (ontapi) al più recente raccoglitore REST ONTAP , procedere come segue:

1. Aggiungere il REST Collector. Si consiglia di immettere le informazioni per un utente diverso da quello configurato per il raccoglitore precedente. Ad esempio, utilizzare l'utente indicato nella sezione Autorizzazioni sopra.
2. Mette in pausa il raccoglitore precedente, in modo che non continui a raccogliere dati.
3. Lasciare che il nuovo collettore REST acquisisca i dati per almeno 30 minuti. Ignorare tutti i dati che durante questo periodo non sembrano "normali".
4. Dopo il periodo di riposo, dovresti vedere i tuoi dati stabilizzarsi mentre il collettore REST continua ad acquisire.

Se lo desideri, puoi usare lo stesso procedimento per tornare al collettore precedente.

Configurazione

Campo	Descrizione
Indirizzo IP di gestione ONTAP	Indirizzo IP o nome di dominio completo del cluster NetApp . Deve essere l'IP/FQDN di gestione del cluster.
Nome utente ONTAP REST	Nome utente per il cluster NetApp
Password ONTAP REST	Password per il cluster NetApp

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti.
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 60 secondi.
Raccolta dati avanzata del contatore	Selezionare questa opzione per includere i dati del contatore avanzato ONTAP nei sondaggi. Abilitato per impostazione predefinita.
Abilita raccolta eventi EMS	Selezionare questa opzione per includere i dati degli eventi del registro ONTAP EMS. Abilitato per impostazione predefinita.
Intervallo di interrogazione EMS (sec)	Il valore predefinito è 60 secondi.

Terminologia

Data Infrastructure Insights acquisisce dati di inventario, registri e prestazioni dal raccoglitore dati ONTAP . Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per l'asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Gruppo di incursione	Gruppo di dischi
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
Aggregato	Pool di archiviazione
LUN	Volume
Volume	Volume interno
Macchina virtuale di archiviazione/Vserver	Macchina virtuale di archiviazione

Terminologia di gestione dei dati ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle pagine di destinazione delle risorse di archiviazione ONTAP Data Management. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

Magazzinaggio

- Modello: elenco delimitato da virgole dei nomi univoci e discreti dei modelli di nodi all'interno di questo cluster. Se tutti i nodi nei cluster sono dello stesso tipo di modello, verrà visualizzato un solo nome di modello.
- Fornitore: lo stesso nome del fornitore che vedresti se stessi configurando una nuova origine dati.
- Numero di serie: l'UUID dell'array
- IP: in genere saranno gli IP o i nomi host configurati nell'origine dati.
- Versione del microcodice – firmware.
- Capacità grezza: somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo.
- Latenza: rappresentazione di ciò che sta sperimentando l'host sottoposto a carichi di lavoro, sia in lettura che in scrittura. Idealmente, Data Infrastructure Insights reperirebbe questo valore direttamente, ma spesso non è così. Invece dell'array che offre questa funzionalità, Data Infrastructure Insights esegue in genere un calcolo ponderato in base agli IOPS derivato dalle statistiche dei singoli volumi interni.
- Capacità di elaborazione: aggregata dai volumi interni. Gestione: può contenere un collegamento ipertestuale all'interfaccia di gestione del dispositivo. Creato a livello di programmazione dalla fonte dati Data Infrastructure Insights come parte della reportistica di inventario.

Pool di archiviazione

- Archiviazione: su quale array di archiviazione risiede questo pool. Obbligatorio.
- Tipo: un valore descrittivo da un elenco di possibilità enumerate. Nella maggior parte dei casi sarà "Aggregato" o "Gruppo RAID".
- Nodo: se l'architettura di questo array di archiviazione è tale che i pool appartengono a un nodo di archiviazione specifico, il suo nome verrà visualizzato qui come collegamento ipertestuale alla relativa landing page.
- Utilizza Flash Pool – Valore Sì/No – questo pool basato su SATA/SAS ha SSD utilizzati per l'accelerazione della memorizzazione nella cache?
- Ridondanza: livello RAID o schema di protezione. RAID_DP è a doppia parità, RAID_TP è a tripla parità.
- Capacità: i valori qui indicati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata tra queste.
- Capacità sovraimpegnata: se utilizzando tecnologie di efficienza è stata assegnata una somma totale di volume o capacità di volume interno superiore alla capacità logica del pool di archiviazione, il valore percentuale sarà maggiore dello 0%.
- Snapshot: capacità di snapshot utilizzate e totali, se l'architettura del pool di archiviazione dedica parte della sua capacità ad aree di segmenti esclusivamente per gli snapshot. È probabile che le configurazioni ONTAP in MetroCluster presentino questo fenomeno, mentre altre configurazioni ONTAP lo presentano in misura minore.
- Utilizzo: valore percentuale che indica la percentuale più alta di disco occupato tra tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. L'utilizzo del disco non ha necessariamente una forte correlazione con le prestazioni dell'array: l'utilizzo può essere elevato a causa di ricostruzioni del disco, attività di deduplicazione, ecc. in assenza di carichi di lavoro gestiti dall'host. Inoltre, molte implementazioni di replicazione degli array possono aumentare l'utilizzo del disco senza essere visualizzate come volume interno o carico di lavoro del volume.
- IOPS: la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Throughput: la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione.

Nodo di archiviazione

- Archiviazione: di quale array di archiviazione fa parte questo nodo. Obbligatorio.
- Partner HA: sulle piattaforme in cui un nodo esegue il failover su un solo altro nodo, in genere verrà visualizzato qui.
- Stato: salute del nodo. Disponibile solo quando l'array è sufficientemente integro da poter essere inventariato da una fonte dati.
- Modello: nome del modello del nodo.
- Versione: nome della versione del dispositivo.
- Numero di serie: il numero di serie del nodo.
- Memoria: memoria base 2 se disponibile.
- Utilizzo: su ONTAP, si tratta di un indice di stress del controller derivante da un algoritmo proprietario. A ogni sondaggio sulle prestazioni verrà segnalato un numero compreso tra 0 e 100%, che rappresenta il valore più alto tra la contesa del disco WAFL o l'utilizzo medio della CPU. Se si osservano valori sostenuti > 50%, ciò è indicativo di sottodimensionamento, ovvero un controller/nodo non sufficientemente grande o un numero insufficiente di dischi rotanti per assorbire il carico di lavoro di scrittura.
- IOPS – Derivato direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Latenza: derivata direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Throughput: derivato direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Processori: numero di CPU.

Metriche di potenza ONTAP

Diversi modelli ONTAP forniscono metriche di potenza per Data Infrastructure Insights che possono essere utilizzate per il monitoraggio o l'invio di avvisi. Gli elenchi dei modelli supportati e non supportati riportati di seguito non sono esaustivi, ma dovrebbero fornire alcune indicazioni; in generale, se un modello appartiene alla stessa famiglia di uno presente nell'elenco, il supporto dovrebbe essere lo stesso.

Modelli supportati:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelli non supportati:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Problema:	Prova questo:
Quando si tenta di creare un raccoglitore di dati REST ONTAP , viene visualizzato un errore simile al seguente: Configurazione: 10.193.70.14: l'API REST ONTAP su 10.193.70.14 non è disponibile: 10.193.70.14 non è riuscito a GET /api/cluster: 400 Richiesta non valida	Ciò è probabilmente dovuto a un array ONTAP più vecchio (ad esempio ONTAP 9.6) che non ha funzionalità API REST. ONTAP 9.14.1 è la versione minima ONTAP supportata dal collettore REST ONTAP . Nelle versioni precedenti a REST ONTAP ci si dovrebbe aspettare risposte "400 Bad Request". Per le versioni ONTAP che supportano REST ma non sono 9.14.1 o successive, potrebbe essere visualizzato il seguente messaggio simile: Configurazione: 10.193.98.84: l'API REST ONTAP su 10.193.98.84 non è disponibile: 10.193.98.84: l'API REST ONTAP su 10.193.98.84 è disponibile: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ma non è della versione minima 9.14.1.
Vedo metriche vuote o "0" dove il collettore ONTAP ontapi mostra i dati.	ONTAP REST non segnala metriche utilizzate internamente solo sul sistema ONTAP . Ad esempio, gli aggregati di sistema non verranno raccolti da ONTAP REST, ma solo gli SVM di tipo "dati". Altri esempi di metriche ONTAP REST che potrebbero segnalare dati pari a zero o vuoti: InternalVolumes: REST non segnala più vol0. Aggregati: REST non segnala più aggr0. Archiviazione: la maggior parte delle metriche è un riepilogo delle metriche del volume interno e sarà influenzata da quanto sopra. Macchine virtuali di archiviazione: REST non segnala più SVM di tipo diverso da "dati" (ad esempio "cluster", "mgmt", "nodo"). Potresti anche notare un cambiamento nell'aspetto dei grafici che contengono dati, dovuto alla modifica del periodo di polling delle prestazioni predefinito da 15 a 5 minuti. Sondaggi più frequenti significano più punti dati da tracciare.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Software di gestione dati NetApp ONTAP, raccoglitore di dati

Questo raccoglitore di dati acquisisce dati di inventario e prestazioni dai sistemi di archiviazione che eseguono ONTAP utilizzando chiamate API di sola lettura da un account ONTAP . Questo raccoglitore di dati crea anche un record nel registro delle applicazioni del cluster per accelerare il supporto.

Terminologia

Data Infrastructure Insights acquisisce dati di inventario e prestazioni dal raccoglitore dati ONTAP . Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per l'asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Gruppo di incursione	Gruppo di dischi
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
Aggregato	Pool di archiviazione
LUN	Volume
Volume	Volume interno

Terminologia di gestione dei dati ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle pagine di destinazione delle risorse di archiviazione ONTAP Data Management. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

Magazzinaggio

- Modello: elenco delimitato da virgole dei nomi univoci e discreti dei modelli di nodi all'interno di questo cluster. Se tutti i nodi nei cluster sono dello stesso tipo di modello, verrà visualizzato un solo nome di modello.
- Fornitore: lo stesso nome del fornitore che vedresti se stessi configurando una nuova origine dati.
- Numero di serie: il numero di serie dell'array. Nei sistemi di archiviazione con architettura cluster come ONTAP Data Management, questo numero di serie potrebbe essere meno utile dei numeri di serie dei singoli "Storage Nodes".
- IP: in genere saranno gli IP o i nomi host configurati nell'origine dati.
- Versione del microcodice – firmware.
- Capacità grezza: somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo.
- Latenza: rappresentazione di ciò che sta sperimentando l'host sottoposto a carichi di lavoro, sia in lettura che in scrittura. Idealmente, Data Infrastructure Insights reperirebbe questo valore direttamente, ma spesso non è così. Invece dell'array che offre questa funzionalità, Data Infrastructure Insights esegue in genere un calcolo ponderato in base agli IOPS derivato dalle statistiche dei singoli volumi interni.
- Capacità di elaborazione: aggregata dai volumi interni. Gestione: può contenere un collegamento ipertestuale all'interfaccia di gestione del dispositivo. Creato a livello di programmazione dalla fonte dati Data Infrastructure Insights come parte della reportistica di inventario.

Pool di archiviazione

- Archiviazione: su quale array di archiviazione risiede questo pool. Obbligatorio.
- Tipo: un valore descrittivo da un elenco di possibilità enumerate. Nella maggior parte dei casi sarà "Aggregato" o "Gruppo RAID".
- Nodo: se l'architettura di questo array di archiviazione è tale che i pool appartengono a un nodo di archiviazione specifico, il suo nome verrà visualizzato qui come collegamento ipertestuale alla relativa landing page.
- Utilizza Flash Pool – Valore Sì/No – questo pool basato su SATA/SAS ha SSD utilizzati per l'accelerazione della memorizzazione nella cache?

- Ridondanza: livello RAID o schema di protezione. RAID_DP è a doppia parità, RAID_TP è a tripla parità.
- Capacità: i valori qui indicati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata tra queste.
- Capacità sovraimpegnata: se utilizzando tecnologie di efficienza è stata assegnata una somma totale di volume o capacità di volume interno superiore alla capacità logica del pool di archiviazione, il valore percentuale sarà maggiore dello 0%.
- Snapshot: capacità di snapshot utilizzate e totali, se l'architettura del pool di archiviazione dedica parte della sua capacità ad aree di segmenti esclusivamente per gli snapshot. È probabile che le configurazioni ONTAP in MetroCluster presentino questo fenomeno, mentre altre configurazioni ONTAP lo presentano in misura minore.
- Utilizzo: valore percentuale che indica la percentuale più alta di disco occupato tra tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. L'utilizzo del disco non ha necessariamente una forte correlazione con le prestazioni dell'array: l'utilizzo può essere elevato a causa di ricostruzioni del disco, attività di deduplicazione, ecc. in assenza di carichi di lavoro gestiti dall'host. Inoltre, molte implementazioni di replicazione degli array possono aumentare l'utilizzo del disco senza essere visualizzate come volume interno o carico di lavoro del volume.
- IOPS: la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Throughput: la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione.

Nodo di archiviazione

- Archiviazione: di quale array di archiviazione fa parte questo nodo. Obbligatorio.
- Partner HA: sulle piattaforme in cui un nodo esegue il failover su un solo altro nodo, in genere verrà visualizzato qui.
- Stato: salute del nodo. Disponibile solo quando l'array è sufficientemente integro da poter essere inventariato da una fonte dati.
- Modello: nome del modello del nodo.
- Versione: nome della versione del dispositivo.
- Numero di serie: il numero di serie del nodo.
- Memoria: memoria base 2 se disponibile.
- Utilizzo: su ONTAP, si tratta di un indice di stress del controller derivante da un algoritmo proprietario. A ogni sondaggio sulle prestazioni verrà segnalato un numero compreso tra 0 e 100%, che rappresenta il valore più alto tra la contesa del disco WAFL o l'utilizzo medio della CPU. Se si osservano valori sostenuti > 50%, ciò è indicativo di sottodimensionamento, ovvero un controller/nodo non sufficientemente grande o un numero insufficiente di dischi rotanti per assorbire il carico di lavoro di scrittura.
- IOPS – Derivato direttamente dalle chiamate ONTAP ZAPI sull'oggetto nodo.
- Latenza: derivata direttamente dalle chiamate ONTAP ZAPI sull'oggetto nodo.
- Throughput: derivato direttamente dalle chiamate ONTAP ZAPI sull'oggetto nodo.
- Processori: numero di CPU.

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questo raccoglitore dati:

- È necessario disporre dell'accesso a un account amministratore configurato per le chiamate API di sola lettura.

- I dettagli dell'account includono nome utente e password.
- Requisiti della porta: 80 o 443
- Autorizzazioni dell'account:
  - Nome del ruolo di sola lettura per l'applicazione ontapi sul Vserver predefinito
  - Potrebbero essere necessari permessi di scrittura facoltativi aggiuntivi. Vedere la Nota sulle autorizzazioni qui sotto.
- Requisiti per la licenza ONTAP :
  - Licenza FCP e volumi mappati/mascherati richiesti per la scoperta del canale in fibra

Requisiti di autorizzazione per la raccolta delle metriche dello switch ONTAP

Data Infrastructure Insights ha la capacità di raccogliere dati sullo switch del cluster ONTAP come opzione nel collettoreConfigurazione avanzata impostazioni. Oltre ad abilitare questa funzionalità sul raccoglitore Data Infrastructure Insights , è necessario anche *configurare il sistema ONTAP * stesso per fornire"informazioni sullo switch" e garantire la correttapermessi sono impostati per consentire l'invio dei dati dello switch a Data Infrastructure Insights.

Configurazione

Campo	Descrizione
IP di gestione NetApp	Indirizzo IP o nome di dominio completo del cluster NetApp
Nome utente	Nome utente per il cluster NetApp
Password	Password per il cluster NetApp

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	Scegli HTTP (porta predefinita 80) o HTTPS (porta predefinita 443). L'impostazione predefinita è HTTPS
Sostituisci porta di comunicazione	Specificare una porta diversa se non si desidera utilizzare quella predefinita
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti.
Per TLS per HTTPS	Consenti TLS come protocollo solo quando si utilizza HTTPS
Ricerca automatica dei netgroup	Abilita le ricerche automatiche di netgroup per le regole dei criteri di esportazione
Espansione di Netgroup	Strategia di espansione di Netgroup. Scegli *file* o *shell*. L'impostazione predefinita è *shell*.
Timeout di lettura HTTP in secondi	Il valore predefinito è 30
Forza le risposte come UTF-8	Forza il codice del raccoglitore dati a interpretare le risposte dalla CLI come se fossero in UTF-8
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 900 secondi.

Campo	Descrizione
Raccolta dati avanzata del contatore	Abilita l'integrazione ONTAP . Selezionare questa opzione per includere i dati del contatore avanzato ONTAP nei sondaggi. Selezionare i contatori desiderati dall'elenco.
Metriche di commutazione del cluster	Consenti a Data Infrastructure Insights di raccogliere i dati dello switch del cluster. Si noti che oltre ad abilitare questa funzionalità sul lato Data Infrastructure Insights , è necessario configurare anche il sistema ONTAP per fornire"informazioni sullo switch" e garantire la correttapermessi sono impostati per consentire l'invio dei dati dello switch a Data Infrastructure Insights. Vedere "Nota sulle autorizzazioni" di seguito.

Metriche di potenza ONTAP

Diversi modelli ONTAP forniscono metriche di potenza per Data Infrastructure Insights che possono essere utilizzate per il monitoraggio o l'invio di avvisi.

Questi elenchi non sono esaustivi e sono soggetti a modifiche. In generale, se un modello appartiene alla stessa famiglia di un altro nell'elenco, il supporto dovrebbe essere lo stesso, ma non è garantito che lo sia. Se non sei sicuro che il tuo modello supporti le metriche di potenza, contatta l'assistenza ONTAP .

Modelli supportati:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelli non supportati:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Una nota sui permessi

Poiché numerose dashboard ONTAP di Data Infrastructure Insights si basano su contatori ONTAP avanzati, è necessario abilitare la **Raccolta dati contatore avanzata** nella sezione Configurazione avanzata del raccoglitore dati.

È inoltre necessario assicurarsi che sia abilitata l'autorizzazione di scrittura per l'API ONTAP . In genere è necessario un account a livello di cluster con le autorizzazioni necessarie.

Per creare un account locale per Data Infrastructure Insights a livello di cluster, accedere a ONTAP con il nome utente/password dell'amministratore di gestione del cluster ed eseguire i seguenti comandi sul server ONTAP :

1. Prima di iniziare, è necessario aver effettuato l'accesso a ONTAP con un account *Amministratore* e i *comandi a livello diagnostico* devono essere abilitati.
2. Creare un ruolo di sola lettura utilizzando i seguenti comandi.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. Creare l'utente di sola lettura utilizzando il seguente comando. Dopo aver eseguito il comando create, ti verrà chiesto di immettere una password per questo utente.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

Se viene utilizzato un account AD/LDAP, il comando deve essere

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Se si raccolgono dati sullo switch del cluster:
```

```
security login rest-role create -role ci_readonly_rest -api
/api/network/ethernet -access readonly
security login create -user-or-group-name ci_user -application http
-authmethod password -role ci_readonly_rest
```

Il ruolo risultante e l'accesso utente saranno simili ai seguenti. Il risultato effettivo potrebbe variare:

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------ --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1:security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

Se il controllo di accesso ONTAP non è impostato correttamente, le chiamate REST Data Infrastructure Insights potrebbero non riuscire, causando lacune nei dati per il dispositivo. Ad esempio, se è stato abilitato sul raccoglitore Data Infrastructure Insights ma non sono state configurate le autorizzazioni su ONTAP, l'acquisizione non andrà a buon fine. Inoltre, se il ruolo è stato precedentemente definito ONTAP e si stanno aggiungendo le funzionalità dell'API REST, assicurarsi che *http* sia aggiunto al ruolo.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Ricevi la risposta HTTP 401 o il codice di errore ZAPI 13003 e ZAPI restituisce "Privilegi insufficienti" o "non autorizzato per questo comando"	Controllare nome utente, password e privilegi/permessi dell'utente.
La versione del cluster è < 8.1	La versione minima supportata dal cluster è 8.1. Aggiorna alla versione minima supportata.
ZAPI restituisce "il ruolo del cluster non è cluster_mgmt LIF"	L'AU deve comunicare con l'IP di gestione del cluster. Controllare l'IP e, se necessario, cambiarlo con un IP diverso
Errore: "I filtri in modalità 7 non sono supportati"	Ciò può accadere se si utilizza questo raccoglitore di dati per scoprire il filtro in modalità 7. Cambiare l'IP in modo che punti al cluster cdot.
Il comando ZAPI fallisce dopo il nuovo tentativo	L'AU ha problemi di comunicazione con il cluster. Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare a eseguire un comando dalla riga di comando della macchina AU.
AU non è riuscito a connettersi a ZAPI tramite HTTP	Verificare se la porta ZAPI accetta testo in chiaro. Se AU tenta di inviare testo in chiaro a un socket SSL, la comunicazione fallisce.
La comunicazione fallisce con SSLException	AU sta tentando di inviare SSL a una porta in chiaro su un filer. Verificare se la porta ZAPI accetta SSL oppure utilizzare una porta diversa.
Errori di connessione aggiuntivi: la risposta ZAPI ha il codice di errore 13001, "database non aperto". Il codice di errore ZAPI è 60 e la risposta contiene "API non completata in tempo". La risposta ZAPI contiene "initialize_session() ha restituito ambiente NULL". Il codice di errore ZAPI è 14007 e la risposta contiene "Nodo non funzionante".	Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare a eseguire un comando dalla riga di comando della macchina AU.

Prestazione

Problema:	Prova questo:
Errore "Impossibile raccogliere le prestazioni da ZAPI"	Di solito ciò è dovuto al fatto che la statistica delle prestazioni non è in esecuzione. Prova il seguente comando su ciascun nodo: > *system node systemshell -node * -command “spmctl -h cmd –stop; spmctl -h cmd –exec”*

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati REST NetApp ONTAP

Questo raccoglitore di dati acquisisce dati di inventario, registri EMS e dati sulle prestazioni dai sistemi di archiviazione che eseguono ONTAP 9.14.1 e versioni successive utilizzando chiamate API REST. Per i sistemi ONTAP nelle versioni precedenti, utilizzare il tipo di collettore "NetApp ONTAP Data Management Software" basato su ZAPI.

Il collettore REST ONTAP può essere utilizzato in sostituzione del precedente collettore basato su ONTAPI. Pertanto, potrebbero esserci differenze nelle metriche raccolte o segnalate. Per ulteriori informazioni sulle differenze tra ONTAPI e REST, vedere"ONTAP 9.14.1 Mapping ONTAPI-REST" documentazione.

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questo raccoglitore dati:

- È necessario avere accesso a un account utente con il livello di accesso richiesto. Si noti che sono necessarie le autorizzazioni di amministratore se si crea un nuovo utente/ruolo REST.
  - Dal punto di vista funzionale, Data Infrastructure Insights esegue principalmente richieste di lettura, ma sono necessarie alcune autorizzazioni di scrittura affinché Data Infrastructure Insights possa registrarsi con l’array ONTAP . Vedere la *Nota sulle autorizzazioni* subito sotto.
- ONTAP versione 9.14.1 o successiva.
- Requisiti della porta: 443
- Si noti che le metriche Fpolicy non sono supportate nel raccoglitore REST ONTAP (i raccoglitori dati Workload Security utilizzano server FPolicy e le metriche FPolicy consentono di monitorare l’attività di raccolta dati Workload Security). Per supportare le metriche Fpolicy, utilizzare "Gestione dei dati ONTAP" collettore.

Una nota sui permessi

Poiché numerose dashboard ONTAP di Data Infrastructure Insights si basano su contatori ONTAP avanzati, è consigliabile mantenere abilitata l’opzione **Abilita raccolta dati contatore avanzata** nella sezione Configurazione avanzata del raccoglitore dati.

Per creare un account locale per Data Infrastructure Insights a livello di cluster, accedere a ONTAP con il nome utente/password dell’amministratore di gestione del cluster ed eseguire i seguenti comandi sul server ONTAP :

1. Prima di iniziare, è necessario aver effettuato l’accesso a ONTAP con un account *Amministratore* e i *comandi a livello diagnostico* devono essere abilitati.

2. Recupera il nome del vserver di tipo *admin*. Utilizzerai questo nome nei comandi successivi.

```
 vserver show -type admin
. Crea un ruolo utilizzando i seguenti comandi:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
```

3. Creare l'utente di sola lettura utilizzando il seguente comando. Dopo aver eseguito il comando create, ti verrà chiesto di immettere una password per questo utente. Si noti che nel comando seguente mostriamo il ruolo impostato su *ci_readonly*. Se nel passaggio 3 sopra riportato si crea un ruolo con un nome diverso, utilizzare al suo posto il nome personalizzato del ruolo.

```
 security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
Se viene utilizzato un account AD/LDAP, il comando deve essere
```

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Il ruolo risultante e l'accesso utente saranno simili ai seguenti.  Il
risultato effettivo potrebbe variare:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   -------------------     ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Se necessario, puoi verificare l'accesso spi:

```
**Vserver:> vserver services web access show -name spi
 Vserver                      Type     Service Name     Role
-------------- -------- ---------------- ----------------
<vserver name >     admin             spi           admin
<vserver name >     admin             spi           csrestrole

2 entries were displayed.**
```

Migrazione

Per migrare da un precedente raccoglitore dati ONTAP (ontapi) al più recente raccoglitore REST ONTAP , procedere come segue:

1. Aggiungere il REST Collector. Si consiglia di immettere le informazioni per un utente diverso da quello configurato per il raccoglitore precedente. Ad esempio, utilizzare l'utente indicato nella sezione Autorizzazioni sopra.
2. Mette in pausa il raccoglitore precedente, in modo che non continui a raccogliere dati.
3. Lasciare che il nuovo collettore REST acquisisca i dati per almeno 30 minuti. Ignorare tutti i dati che durante questo periodo non sembrano "normali".
4. Dopo il periodo di riposo, dovresti vedere i tuoi dati stabilizzarsi mentre il collettore REST continua ad acquisire.

Se lo desideri, puoi usare lo stesso procedimento per tornare al collettore precedente.

Configurazione

Campo	Descrizione
Indirizzo IP di gestione ONTAP	Indirizzo IP o nome di dominio completo del cluster NetApp . Deve essere l'IP/FQDN di gestione del cluster.
Nome utente ONTAP REST	Nome utente per il cluster NetApp
Password ONTAP REST	Password per il cluster NetApp

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti.
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 60 secondi.
Raccolta dati avanzata del contatore	Selezionare questa opzione per includere i dati del contatore avanzato ONTAP nei sondaggi. Abilitato per impostazione predefinita.
Abilita raccolta eventi EMS	Selezionare questa opzione per includere i dati degli eventi del registro ONTAP EMS. Abilitato per impostazione predefinita.
Intervallo di interrogazione EMS (sec)	Il valore predefinito è 60 secondi.

Terminologia

Data Infrastructure Insights acquisisce dati di inventario, registri e prestazioni dal raccoglitore dati ONTAP . Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per l'asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Gruppo di incursione	Gruppo di dischi
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
Aggregato	Pool di archiviazione
LUN	Volume
Volume	Volume interno
Macchina virtuale di archiviazione/Vserver	Macchina virtuale di archiviazione

Terminologia di gestione dei dati ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle pagine di destinazione delle risorse di archiviazione ONTAP Data Management. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

Magazzinaggio

- Modello: elenco delimitato da virgole dei nomi univoci e discreti dei modelli di nodi all'interno di questo cluster. Se tutti i nodi nei cluster sono dello stesso tipo di modello, verrà visualizzato un solo nome di modello.
- Fornitore: lo stesso nome del fornitore che vedresti se stessi configurando una nuova origine dati.
- Numero di serie: l'UUID dell'array
- IP: in genere saranno gli IP o i nomi host configurati nell'origine dati.
- Versione del microcodice – firmware.
- Capacità grezza: somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo.
- Latenza: rappresentazione di ciò che sta sperimentando l'host sottoposto a carichi di lavoro, sia in lettura che in scrittura. Idealmente, Data Infrastructure Insights reperirebbe questo valore direttamente, ma spesso non è così. Invece dell'array che offre questa funzionalità, Data Infrastructure Insights esegue in genere un calcolo ponderato in base agli IOPS derivato dalle statistiche dei singoli volumi interni.
- Capacità di elaborazione: aggregata dai volumi interni. Gestione: può contenere un collegamento ipertestuale all'interfaccia di gestione del dispositivo. Creato a livello di programmazione dalla fonte dati Data Infrastructure Insights come parte della reportistica di inventario.

Pool di archiviazione

- Archiviazione: su quale array di archiviazione risiede questo pool. Obbligatorio.
- Tipo: un valore descrittivo da un elenco di possibilità enumerate. Nella maggior parte dei casi sarà "Aggregato" o "Gruppo RAID".
- Nodo: se l'architettura di questo array di archiviazione è tale che i pool appartengono a un nodo di archiviazione specifico, il suo nome verrà visualizzato qui come collegamento ipertestuale alla relativa landing page.
- Utilizza Flash Pool – Valore Sì/No – questo pool basato su SATA/SAS ha SSD utilizzati per l'accelerazione della memorizzazione nella cache?
- Ridondanza: livello RAID o schema di protezione. RAID_DP è a doppia parità, RAID_TP è a tripla parità.
- Capacità: i valori qui indicati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata tra queste.
- Capacità sovraimpegnata: se utilizzando tecnologie di efficienza è stata assegnata una somma totale di volume o capacità di volume interno superiore alla capacità logica del pool di archiviazione, il valore percentuale sarà maggiore dello 0%.
- Snapshot: capacità di snapshot utilizzate e totali, se l'architettura del pool di archiviazione dedica parte della sua capacità ad aree di segmenti esclusivamente per gli snapshot. È probabile che le configurazioni ONTAP in MetroCluster presentino questo fenomeno, mentre altre configurazioni ONTAP lo presentano in misura minore.
- Utilizzo: valore percentuale che indica la percentuale più alta di disco occupato tra tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. L'utilizzo del disco non ha necessariamente una forte correlazione con le prestazioni dell'array: l'utilizzo può essere elevato a causa di ricostruzioni del disco, attività di deduplicazione, ecc. in assenza di carichi di lavoro gestiti dall'host. Inoltre, molte implementazioni di replicazione degli array possono aumentare l'utilizzo del disco senza essere visualizzate come volume interno o carico di lavoro del volume.
- IOPS: la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Throughput: la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione.

Nodo di archiviazione

- Archiviazione: di quale array di archiviazione fa parte questo nodo. Obbligatorio.
- Partner HA: sulle piattaforme in cui un nodo esegue il failover su un solo altro nodo, in genere verrà visualizzato qui.
- Stato: salute del nodo. Disponibile solo quando l'array è sufficientemente integro da poter essere inventariato da una fonte dati.
- Modello: nome del modello del nodo.
- Versione: nome della versione del dispositivo.
- Numero di serie: il numero di serie del nodo.
- Memoria: memoria base 2 se disponibile.
- Utilizzo: su ONTAP, si tratta di un indice di stress del controller derivante da un algoritmo proprietario. A ogni sondaggio sulle prestazioni verrà segnalato un numero compreso tra 0 e 100%, che rappresenta il valore più alto tra la contesa del disco WAFL o l'utilizzo medio della CPU. Se si osservano valori sostenuti > 50%, ciò è indicativo di sottodimensionamento, ovvero un controller/nodo non sufficientemente grande o un numero insufficiente di dischi rotanti per assorbire il carico di lavoro di scrittura.
- IOPS – Derivato direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Latenza: derivata direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Throughput: derivato direttamente dalle chiamate ONTAP REST sull'oggetto nodo.
- Processori: numero di CPU.

Metriche di potenza ONTAP

Diversi modelli ONTAP forniscono metriche di potenza per Data Infrastructure Insights che possono essere utilizzate per il monitoraggio o l'invio di avvisi. Gli elenchi dei modelli supportati e non supportati riportati di seguito non sono esaustivi, ma dovrebbero fornire alcune indicazioni; in generale, se un modello appartiene alla stessa famiglia di uno presente nell'elenco, il supporto dovrebbe essere lo stesso.

Modelli supportati:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelli non supportati:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Problema:	Prova questo:
Quando si tenta di creare un raccoglitore di dati REST ONTAP , viene visualizzato un errore simile al seguente: Configurazione: 10.193.70.14: l'API REST ONTAP su 10.193.70.14 non è disponibile: 10.193.70.14 non è riuscito a GET /api/cluster: 400 Richiesta non valida	Ciò è probabilmente dovuto a un array ONTAP più vecchio (ad esempio ONTAP 9.6) che non ha funzionalità API REST. ONTAP 9.14.1 è la versione minima ONTAP supportata dal collettore REST ONTAP . Nelle versioni precedenti a REST ONTAP ci si dovrebbe aspettare risposte "400 Bad Request". Per le versioni ONTAP che supportano REST ma non sono 9.14.1 o successive, potrebbe essere visualizzato il seguente messaggio simile: Configurazione: 10.193.98.84: l'API REST ONTAP su 10.193.98.84 non è disponibile: 10.193.98.84: l'API REST ONTAP su 10.193.98.84 è disponibile: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ma non è della versione minima 9.14.1.
Vedo metriche vuote o "0" dove il collettore ONTAP ontapi mostra i dati.	ONTAP REST non segnala metriche utilizzate internamente solo sul sistema ONTAP . Ad esempio, gli aggregati di sistema non verranno raccolti da ONTAP REST, ma solo gli SVM di tipo "dati". Altri esempi di metriche ONTAP REST che potrebbero segnalare dati pari a zero o vuoti: InternalVolumes: REST non segnala più vol0. Aggregati: REST non segnala più aggr0. Archiviazione: la maggior parte delle metriche è un riepilogo delle metriche del volume interno e sarà influenzata da quanto sopra. Macchine virtuali di archiviazione: REST non segnala più SVM di tipo diverso da "dati" (ad esempio "cluster", "mgmt", "nodo"). Potresti anche notare un cambiamento nell'aspetto dei grafici che contengono dati, dovuto alla modifica del periodo di polling delle prestazioni predefinito da 15 a 5 minuti. Sondaggi più frequenti significano più punti dati da tracciare.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

NetApp Data ONTAP funzionante nel raccoglitore dati a 7 modalità

Per i sistemi di storage che utilizzano il software Data ONTAP che opera in modalità 7, si utilizza il raccoglitore dati a 7 modalità, che sfrutta la CLI per ottenere dati su capacità e prestazioni.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati NetApp a 7 modalità. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per tale asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Questo raccoglitore di dati è"deprecato" .

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Gruppo di incursione	Gruppo di dischi
Filer	Magazzinaggio
Filer	Nodo di archiviazione
Aggregato	Pool di archiviazione
LUN	Volume
Volume	Volume interno

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare e utilizzare questo raccoglitore dati è necessario quanto segue:

- Indirizzi IP del controller di archiviazione FAS e del partner.
- Porta 443
- Un nome utente e una password di livello amministratore personalizzati per il controller e il controller partner con le seguenti capacità di ruolo per 7-Mode:
  - "api-*": utilizzare questa opzione per consentire a OnCommand Insight di eseguire tutti i comandi API di storage NetApp .
  - "login-http-admin": utilizzare questa opzione per consentire a OnCommand Insight di connettersi allo storage NetApp tramite HTTP.
  - "security-api-vfiler": utilizzare questa opzione per consentire a OnCommand Insight di eseguire i comandi API di archiviazione NetApp per recuperare le informazioni sull'unità vFiler.
  - "cli-options": utilizzare per leggere le opzioni del sistema di archiviazione.
  - "cli-lun": accedi a questi comandi per gestire i LUN. Visualizza lo stato (percorso LUN, dimensione, stato online/offline e stato condiviso) del LUN specificato o della classe di LUN.
  - "cli-df": utilizzare per visualizzare lo spazio libero su disco.
  - "cli-ifconfig": utilizzare per visualizzare le interfacce e gli indirizzi IP.

Configurazione

Campo	Descrizione
Indirizzo del sistema di archiviazione	Indirizzo IP o nome di dominio completo per il sistema di archiviazione NetApp
Nome utente	Nome utente per il sistema di archiviazione NetApp
Password	Password per il sistema di archiviazione NetApp
Indirizzo del partner HA nel cluster	Indirizzo IP o nome di dominio completo per il partner HA
Nome utente del partner HA nel cluster	Nome utente per il partner HA

Campo	Descrizione
Password del file partner HA nel cluster	Password per il partner HA

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20 minuti.
Tipo di connessione	HTTPS o HTTP, visualizza anche la porta predefinita
Sostituisci porta di connessione	Se vuoto, utilizzare la porta predefinita nel campo Tipo di connessione, altrimenti immettere la porta di connessione da utilizzare
Intervallo di sondaggio sulle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Collegamento dei sistemi di stoccaggio

In alternativa all'utilizzo dell'utente amministrativo predefinito per questo raccoglitore dati, è possibile configurare un utente con diritti amministrativi direttamente sui sistemi di archiviazione NetApp , in modo che questo raccoglitore dati possa acquisire dati dai sistemi di archiviazione NetApp .

Per connettersi ai sistemi di storage NetApp è necessario che l'utente specificato al momento dell'acquisizione del pfiler principale (su cui esiste il sistema di storage) soddisfi le seguenti condizioni:

- L'utente deve essere su vfiler0 (root filer/pfiler).

  I sistemi di stoccaggio vengono acquisiti al momento dell'acquisizione del pfiler principale.

- I seguenti comandi definiscono le capacità del ruolo utente:
  - "api-*": utilizzare questa opzione per consentire a Data Infrastructure Insights di eseguire tutti i comandi API di storage NetApp .

    Questo comando è necessario per utilizzare ZAPI.

  - "login-http-admin": utilizzare questa opzione per consentire a Data Infrastructure Insights di connettersi allo storage NetApp tramite HTTP. Questo comando è necessario per utilizzare ZAPI.
  - "security-api-vfiler": utilizzare questa opzione per consentire a Data Infrastructure Insights di eseguire comandi API di storage NetApp per recuperare le informazioni sull'unità vFiler.
  - "cli-options": per il comando "options" e utilizzato per l'IP del partner e le licenze abilitate.
  - "cli-lun": accedi a questi comandi per gestire i LUN. Visualizza lo stato (percorso LUN, dimensione, stato online/offline e stato condiviso) del LUN specificato o della classe di LUN.
  - "cli-df": per i comandi "df -s", "df -r", "df -A -r" e utilizzato per visualizzare lo spazio libero.
  - "cli-ifconfig": per il comando "ifconfig -a" e utilizzato per ottenere l'indirizzo IP del filer.
  - "cli-rdfile": per il comando "rdfile /etc/netgroup" e utilizzato per ottenere i netgroup.
  - "cli-date": per il comando "date" e utilizzato per ottenere la data completa per ottenere copie Snapshot.
  - "cli-snap": per il comando "snap list" e utilizzato per ottenere copie Snapshot.

Se non vengono fornite le autorizzazioni cli-date o cli-snap, l'acquisizione può essere completata, ma le copie Snapshot non vengono segnalate.

Per acquisire correttamente una sorgente dati 7-Mode e non generare avvisi sul sistema di archiviazione, è necessario utilizzare una delle seguenti stringhe di comando per definire i ruoli utente. La seconda stringa elencata qui è una versione semplificata della prima:

- login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-df,cli-lun,cli-ifconfig,cli-date,cli-snap,_
- login-http-admin,api-* ,security-api-vfile,cli-

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Ricevi la risposta HTTP 401 o il codice di errore ZAPI 13003 e ZAPI restituisce "Privilegi insufficienti" o "non autorizzato per questo comando"	Controllare nome utente, password e privilegi/permessi dell'utente.
Errore "Impossibile eseguire il comando"	Verificare se l'utente dispone delle seguenti autorizzazioni sul dispositivo: • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler Verificare inoltre se la versione ONTAP è supportata da Data Infrastructure Insights e verificare se le credenziali utilizzate corrispondono alle credenziali del dispositivo
La versione del cluster è < 8.1	La versione minima supportata dal cluster è 8.1. Aggiorna alla versione minima supportata.
ZAPI restituisce "il ruolo del cluster non è cluster_mgmt LIF"	L'AU deve comunicare con l'IP di gestione del cluster. Controllare l'IP e, se necessario, cambiarlo con un IP diverso
Errore: "I filtri in modalità 7 non sono supportati"	Ciò può accadere se si utilizza questo raccoglitore di dati per scoprire il filtro in modalità 7. Cambiare l'IP in modo che punti al filer cdot.
Il comando ZAPI fallisce dopo il nuovo tentativo	L'AU ha problemi di comunicazione con il cluster. Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare a eseguire un comando dalla riga di comando della macchina AU.
AU non è riuscito a connettersi a ZAPI	Verificare la connettività IP/porta e verificare la configurazione ZAPI.
AU non è riuscito a connettersi a ZAPI tramite HTTP	Verificare se la porta ZAPI accetta testo in chiaro. Se AU tenta di inviare testo in chiaro a un socket SSL, la comunicazione fallisce.
La comunicazione fallisce con SSLException	AU sta tentando di inviare SSL a una porta in chiaro su un filer. Verificare se la porta ZAPI accetta SSL oppure utilizzare una porta diversa.

Problema:	Prova questo:
Errori di connessione aggiuntivi: la risposta ZAPI ha il codice di errore 13001, "database non aperto". Il codice di errore ZAPI è 60 e la risposta contiene "API non completata in tempo". La risposta ZAPI contiene "initialize_session() ha restituito ambiente NULL". Il codice di errore ZAPI è 14007 e la risposta contiene "Nodo non funzionante".	Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare a eseguire un comando dalla riga di comando della macchina AU.
Errore di timeout del socket con ZAPI	Controllare la connettività del filer e/o aumentare il timeout.
Errore "I cluster in modalità C non sono supportati dalla sorgente dati in modalità 7"	Controllare l'IP e modificarlo in un cluster in modalità 7.
Errore "Impossibile connettersi a vFiler"	Verificare che le capacità di acquisizione dell'utente includano almeno quanto segue: api-* security-api-vfiler login-http-admin Verificare che il filer esegua almeno la versione ONTAPI 1.7.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati API NetApp E-Series Legacy Santricity

Il raccoglitore di dati API NetApp E-Series Legacy Santricity raccoglie dati di inventario e prestazioni. Il collettore supporta il firmware 7.x+ utilizzando le stesse configurazioni e segnalando gli stessi dati.

Terminologia

Cloud Insight acquisisce le seguenti informazioni di inventario dal raccoglitore dati NetApp E-Series. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per tale asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Gruppo di volumi	Gruppo di dischi
Array di archiviazione	Magazzinaggio
Controllore	Nodo di archiviazione
Gruppo di volumi	Pool di archiviazione
Volume	Volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Terminologia della serie E (pagina di destinazione)

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle landing page delle risorse

NetApp E-Series. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

Magazzinaggio

- Modello: nome del modello del dispositivo.
- Fornitore: lo stesso nome del fornitore che vedresti se stessi configurando una nuova origine dati
- Numero di serie: il numero di serie dell'array. Nei sistemi di archiviazione con architettura cluster come NetApp Clustered Data Ontap, questo numero di serie potrebbe essere meno utile dei singoli numeri di serie dei "nodi di archiviazione"
- IP: in genere saranno gli IP o i nomi host configurati nell'origine dati
- Versione del microcodice – firmware
- Capacità grezza: somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo
- Latenza: rappresentazione di ciò che sta sperimentando l'host che gestisce i carichi di lavoro, sia in lettura che in scrittura. Idealmente, Data Infrastructure Insights reperirebbe questo valore direttamente, ma spesso non è così. Invece dell'array che offre questa funzionalità, Data Infrastructure Insights esegue in genere un calcolo ponderato in base agli IOPS derivato dalle statistiche dei singoli volumi.
- Throughput: il throughput totale dell'array rivolto all'host. Idealmente, se ottenuto direttamente dall'array, se non disponibile, Data Infrastructure Insights somma la produttività dei volumi per ricavare questo valore
- Gestione: può contenere un collegamento ipertestuale all'interfaccia di gestione del dispositivo. Creato a livello di programmazione dalla fonte Data Infrastructure Insights come parte della reportistica di inventario

Pool di archiviazione

- Archiviazione: su quale array di archiviazione risiede questo pool. Obbligatorio
- Tipo: un valore descrittivo da un elenco di possibilità enumerate. Più comunemente sarà "Thin Provisioning" o "RAID Group"
- Nodo: se l'architettura di questo array di archiviazione è tale che i pool appartengono a un nodo di archiviazione specifico, il suo nome verrà visualizzato qui come collegamento ipertestuale alla sua landing page
- Utilizza Flash Pool – Valore Sì/No
- Ridondanza: livello RAID o schema di protezione. E-Series segnala "RAID 7" per i pool DDP
- Capacità: i valori qui indicati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata tra queste. Entrambi questi valori includono la capacità di "conservazione" della Serie E, risultando in numeri e percentuali superiori a quanto potrebbe mostrare l'interfaccia utente della Serie E stessa
- Capacità sovraimpegnata: se tramite tecnologie di efficienza è stata assegnata una somma totale di volume o capacità di volume interno superiore alla capacità logica del pool di archiviazione, il valore percentuale sarà maggiore dello 0%.
- Snapshot: capacità snapshot utilizzate e totali, se l'architettura del pool di archiviazione dedica parte della sua capacità ad aree di segmenti esclusivamente per gli snapshot
- Utilizzo: valore percentuale che indica la percentuale più alta di disco occupato tra tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. L'utilizzo del disco non ha necessariamente una forte correlazione con le prestazioni dell'array: l'utilizzo può essere elevato a causa di ricostruzioni del disco, attività di deduplicazione, ecc. in assenza di carichi di lavoro gestiti dall'host. Inoltre, molte implementazioni di replicazione degli array possono aumentare l'utilizzo del disco senza essere visualizzate come carico di lavoro del volume.

- IOPS: la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Se gli IOPS del disco non sono disponibili su una determinata piattaforma, questo valore verrà ricavato dalla somma degli IOPS del volume per tutti i volumi presenti su questo pool di archiviazione
- Throughput: la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Se la capacità di elaborazione del disco non è disponibile su una determinata piattaforma, questo valore verrà ricavato dalla somma del volume per tutti i volumi presenti su questo pool di archiviazione

Nodo di archiviazione

- Archiviazione: di quale array di archiviazione fa parte questo nodo. Obbligatorio
- Partner HA: sulle piattaforme in cui un nodo eseguirà il failover su un solo altro nodo, generalmente verrà visualizzato qui
- Stato: salute del nodo. Disponibile solo quando l'array è sufficientemente integro da poter essere inventariato da una fonte dati
- Modello: nome del modello del nodo
- Versione: nome della versione del dispositivo.
- Numero di serie: il numero di serie del nodo
- Memoria – memoria base 2 se disponibile
- Utilizzo: in genere un numero di utilizzo della CPU o, nel caso di NetApp Ontap, un indice di stress del controller. L'utilizzo non è attualmente disponibile per NetApp E-Series
- IOPS: numero che rappresenta gli IOPS gestiti dall'host su questo controller. Idealmente, l'origine è direttamente dall'array; se non disponibile, verrà calcolato sommando tutti gli IOPS per i volumi che appartengono esclusivamente a questo nodo.
- Latenza: numero che rappresenta la latenza tipica dell'host o il tempo di risposta su questo controller. Idealmente, l'origine è direttamente dall'array; se non disponibile, verrà calcolato eseguendo un calcolo ponderato degli IOP dai volumi che appartengono esclusivamente a questo nodo.
- Throughput: numero che rappresenta il throughput gestito dall'host su questo controller. Idealmente, la fonte dovrebbe essere direttamente l'array; se non disponibile, verrà calcolato sommando tutta la produttività dei volumi che appartengono esclusivamente a questo nodo.
- Processori – numero di CPU

Requisiti

- L'indirizzo IP di ciascun controller sull'array
- Requisito di porta 2463

Configurazione

Campo	Descrizione
Elenco separato da virgole degli IP del controller Array SANtricity	Indirizzi IP e/o nomi di dominio completi per i controller di array

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 30 minuti
Intervallo di sondaggio delle prestazioni fino a 3600 secondi	Il valore predefinito è 300 secondi

Risoluzione dei problemi

Ulteriori informazioni su questo raccoglitore di dati possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati REST NetApp E-Series

Il raccoglitore di dati REST NetApp E-Series raccoglie dati di inventario, registri e prestazioni. Il collettore supporta il firmware 7.x+ utilizzando le stesse configurazioni e segnalando gli stessi dati. Il collettore REST monitora lo stato di crittografia dei pool di archiviazione, dei dischi e dei volumi, l'utilizzo della CPU del nodo di archiviazione e le funzionalità di registro non fornite nel collettore SANtricity E-Series legacy.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da NetApp E-Series, utilizzando REST. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per tale asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco
Gruppo di volumi	Gruppo di dischi
Array di archiviazione	Magazzinaggio
Controllore	Nodo di archiviazione
Gruppo di volumi	Pool di archiviazione
Volume	Volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- L'indirizzo IP di ciascun controller sull'array
- Questo collettore supporta solo array modello E-Series con **capacità REST API native**. L'organizzazione E-Series fornisce una distribuzione API REST installabile e off-array per i vecchi array E-Series: questo collector non supporta tale scenario. Gli utenti con array più vecchi dovrebbero continuare a utilizzare Data Infrastructure Insights"API SANtricity serie E" collettore.
- Il campo "Indirizzi IP del controller serie E" supporta una stringa delimitata da virgole di 2 IP/nomi host; il raccoglitore proverà in modo intelligente il secondo IP/nome host se il primo non è accessibile.
- Porta HTTPS: l'impostazione predefinita è 8443.

Configurazione

Campo	Descrizione
Indirizzi IP del controller serie E	indirizzi IP separati da virgole e/o nomi di dominio completi per i controller di array

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 30 minuti
Intervallo di sondaggio delle prestazioni fino a 3600 secondi	Il valore predefinito è 300 secondi

Terminologia della serie E (pagina di destinazione)

I seguenti termini si applicano agli oggetti o ai riferimenti che potresti trovare nelle landing page delle risorse NetApp E-Series. Molti di questi termini si applicano anche ad altri raccoglitori di dati.

Magazzinaggio

- Modello: nome del modello del dispositivo.
- Fornitore: lo stesso nome del fornitore che vedresti se stessi configurando una nuova origine dati
- Numero di serie: il numero di serie dell'array. Nei sistemi di archiviazione con architettura cluster come NetApp Clustered Data Ontap, questo numero di serie potrebbe essere meno utile dei singoli numeri di serie dei "nodi di archiviazione"
- IP: in genere saranno gli IP o i nomi host configurati nell'origine dati
- Versione del microcodice – firmware
- Capacità grezza: somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo
- Latenza: rappresentazione di ciò che sta sperimentando l'host che gestisce i carichi di lavoro, sia in lettura che in scrittura. Idealmente, Data Infrastructure Insights reperirebbe questo valore direttamente, ma spesso non è così. Invece dell'array che offre questa funzionalità, Data Infrastructure Insights esegue in genere un calcolo ponderato in base agli IOPS derivato dalle statistiche dei singoli volumi.
- Throughput: il throughput totale dell'array rivolto all'host. Idealmente, se ottenuto direttamente dall'array, se non disponibile, Data Infrastructure Insights somma la produttività dei volumi per ricavare questo valore
- Gestione: può contenere un collegamento ipertestuale all'interfaccia di gestione del dispositivo. Creato a livello di programmazione dalla fonte Data Infrastructure Insights come parte della reportistica di inventario

Pool di archiviazione

- Archiviazione: su quale array di archiviazione risiede questo pool. Obbligatorio
- Tipo: un valore descrittivo da un elenco di possibilità enumerate. Più comunemente sarà "Thin Provisioning" o "RAID Group"
- Nodo: se l'architettura di questo array di archiviazione è tale che i pool appartengono a un nodo di archiviazione specifico, il suo nome verrà visualizzato qui come collegamento ipertestuale alla sua landing page
- Utilizza Flash Pool – Valore Sì/No

- Ridondanza: livello RAID o schema di protezione. E-Series segnala "RAID 7" per i pool DDP
- Capacità: i valori qui indicati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata tra queste. Entrambi questi valori includono la capacità di "conservazione" della Serie E, risultando in numeri e percentuali superiori a quanto potrebbe mostrare l'interfaccia utente della Serie E stessa
- Capacità sovraimpegnata: se tramite tecnologie di efficienza è stata assegnata una somma totale di volume o capacità di volume interno superiore alla capacità logica del pool di archiviazione, il valore percentuale sarà maggiore dello 0%.
- Snapshot: capacità snapshot utilizzate e totali, se l'architettura del pool di archiviazione dedica parte della sua capacità ad aree di segmenti esclusivamente per gli snapshot
- Utilizzo: valore percentuale che indica la percentuale più alta di disco occupato tra tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. L'utilizzo del disco non ha necessariamente una forte correlazione con le prestazioni dell'array: l'utilizzo può essere elevato a causa di ricostruzioni del disco, attività di deduplicazione, ecc. in assenza di carichi di lavoro gestiti dall'host. Inoltre, molte implementazioni di replicazione degli array possono aumentare l'utilizzo del disco senza essere visualizzate come carico di lavoro del volume.
- IOPS: la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Se gli IOPS del disco non sono disponibili su una determinata piattaforma, questo valore verrà ricavato dalla somma degli IOPS del volume per tutti i volumi presenti su questo pool di archiviazione
- Throughput: la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di archiviazione. Se la capacità di elaborazione del disco non è disponibile su una determinata piattaforma, questo valore verrà ricavato dalla somma del volume per tutti i volumi presenti su questo pool di archiviazione

Nodo di archiviazione

- Archiviazione: di quale array di archiviazione fa parte questo nodo. Obbligatorio
- Partner HA: sulle piattaforme in cui un nodo eseguirà il failover su un solo altro nodo, generalmente verrà visualizzato qui
- Stato: salute del nodo. Disponibile solo quando l'array è sufficientemente integro da poter essere inventariato da una fonte dati
- Modello: nome del modello del nodo
- Versione: nome della versione del dispositivo.
- Numero di serie: il numero di serie del nodo
- Memoria – memoria base 2 se disponibile
- Utilizzo: in genere un numero di utilizzo della CPU o, nel caso di NetApp Ontap, un indice di stress del controller. L'utilizzo non è attualmente disponibile per NetApp E-Series
- IOPS: numero che rappresenta gli IOPS gestiti dall'host su questo controller. Idealmente, l'origine è direttamente dall'array; se non disponibile, verrà calcolato sommando tutti gli IOPS per i volumi che appartengono esclusivamente a questo nodo.
- Latenza: numero che rappresenta la latenza tipica dell'host o il tempo di risposta su questo controller. Idealmente, l'origine è direttamente dall'array; se non disponibile, verrà calcolato eseguendo un calcolo ponderato degli IOP dai volumi che appartengono esclusivamente a questo nodo.
- Throughput: numero che rappresenta il throughput gestito dall'host su questo controller. Idealmente, la fonte dovrebbe essere direttamente l'array; se non disponibile, verrà calcolato sommando tutta la produttività dei volumi che appartengono esclusivamente a questo nodo.

- Processori – numero di CPU

Risoluzione dei problemi

Ulteriori informazioni su questo raccoglitore di dati possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati del server di gestione NetApp HCI

Il raccoglitore dati del server di gestione NetApp HCI raccoglie informazioni sull'host NetApp HCI e richiede privilegi di sola lettura su tutti gli oggetti all'interno del server di gestione.

Questo raccoglitore di dati acquisisce solo dal *server di gestione NetApp HCI *. Per raccogliere i dati dal sistema di archiviazione, è necessario configurare anche il"NetApp SolidFire" raccoglitore di dati.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario da questo raccoglitore di dati. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per l'asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco virtuale	Disco
Ospite	Ospite
Macchina virtuale	Macchina virtuale
Archivio dati	Archivio dati
LUN	Volume
Porta Fibre Channel	Porta

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni:

- Indirizzo IP del server di gestione NetApp HCI
- Nome utente e password di sola lettura per il server NetApp HCI Management
- Privilegi di sola lettura su tutti gli oggetti nel server NetApp HCI Management.
- Accesso SDK sul server NetApp HCI Management, solitamente già configurato.
- Requisiti della porta: http-80 https-443
- Convalida l'accesso:
  - Accedi al server NetApp HCI Management utilizzando il nome utente e la password sopra indicati
  - Verifica SDK abilitato: telnet <vc_ip> 443

Installazione e connessione

Campo	Descrizione
Nome	Nome univoco per il raccoglitore di dati
Unità di acquisizione	Nome dell'unità di acquisizione

Configurazione

Campo	Descrizione
Cluster di archiviazione NetApp HCI MVIP	Indirizzo IP virtuale di gestione
Nodo di gestione SolidFire (mNode)	Indirizzo IP del nodo di gestione
Nome utente	Nome utente utilizzato per accedere al server NetApp HCI Management
Password	Password utilizzata per accedere al server di gestione NetApp HCI
Nome utente VCenter	Nome utente per VCenter
Password VCenter	Password per VCenter

Configurazione avanzata

Nella schermata di configurazione avanzata, seleziona la casella **Prestazioni VM** per raccogliere i dati sulle prestazioni. La raccolta dell'inventario è abilitata per impostazione predefinita. È possibile configurare i seguenti campi:

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 20
Filtra le VM per	Seleziona CLUSTER, DATACENTER o ESX HOST
Scegli "Escludi" o "Includi" per specificare un elenco	Specificare se includere o escludere le VM
Filtra elenco dispositivi	Elenco di VM da filtrare (separate da virgole o da punto e virgola se nel valore viene utilizzata una virgola) per il filtraggio solo per ESX_HOST, CLUSTER e DATACENTER
Intervallo di sondaggio delle prestazioni (sec)	Il valore predefinito è 300

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: l'elenco da includere per filtrare le VM non può essere vuoto	Se è selezionato Includi elenco, elenca i nomi validi di DataCenter, Cluster o Host per filtrare le VM

Problema:	Prova questo:
Errore: impossibile creare una connessione a VirtualCenter all'IP	Possibili soluzioni: * Verificare le credenziali e l'indirizzo IP immessi. * Prova a comunicare con Virtual Center tramite Infrastructure Client. * Prova a comunicare con Virtual Center utilizzando Managed Object Browser (ad esempio MOB).
Errore: VirtualCenter su IP ha un certificato non conforme richiesto da JVM	Soluzioni possibili: * Consigliato: rigenerare il certificato per Virtual Center utilizzando una chiave RSA più potente (ad esempio a 1024 bit). * Sconsigliato: modificare la configurazione java.security della JVM per sfruttare il vincolo jdk.certpath.disabledAlgorithms per consentire la chiave RSA a 512 bit. Vedere le note di rilascio dell’aggiornamento 40 di JDK 7 su"http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati NetApp SolidFire All-Flash Array

Il raccoglitore di dati NetApp SolidFire All-Flash Array supporta la raccolta di inventario e prestazioni da configurazioni SolidFire sia iSCSI che Fibre Channel.

Il raccoglitore dati SolidFire utilizza la SolidFire REST API. L'unità di acquisizione in cui risiede il raccoglitore dati deve essere in grado di avviare connessioni HTTPS alla porta TCP 443 sull'indirizzo IP di gestione del cluster SolidFire . Il raccoglitore dati necessita di credenziali in grado di effettuare query REST API sul cluster SolidFire .

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati NetApp SolidFire All-Flash Array. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Guidare	Disco
Grappolo	Magazzinaggio
Nodo	Nodo di archiviazione
Volume	Volume
Porta Fibre Channel	Porta
Gruppo di accesso al volume, assegnazione LUN	Mappa del volume
Sessione iSCSI	Maschera del volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questo raccoglitore dati:

- Indirizzo IP virtuale di gestione
- Nome utente e credenziali di sola lettura
- Porta 443

Configurazione

Campo	Descrizione
Indirizzo IP virtuale di gestione (MVIP)	Indirizzo IP virtuale di gestione del cluster SolidFire
Nome utente	Nome utilizzato per accedere al cluster SolidFire
Password	Password utilizzata per accedere al cluster SolidFire

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	Scegli il tipo di connessione
Porta di comunicazione	Porta utilizzata per l'API NetApp
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 20 minuti
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 300 secondi

Risoluzione dei problemi

Quando SolidFire segnala un errore, questo viene visualizzato in Data Infrastructure Insights come segue:

È stato ricevuto un messaggio di errore da un dispositivo SolidFire durante il tentativo di recupero dei dati. La chiamata era <metodo> (<stringaparametro>). Il messaggio di errore del dispositivo era (controllare il manuale del dispositivo): <messaggio>

Dove:

- <metodo> è un metodo HTTP, come GET o PUT.
- <parameterString> è un elenco separato da virgole di parametri inclusi nella chiamata REST.
- Il <messaggio> è qualsiasi cosa il dispositivo abbia restituito come messaggio di errore.

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati NetApp StorageGRID

Il raccoglitore dati NetApp StorageGRID supporta la raccolta di inventario e prestazioni dalle configurazioni StorageGRID .

Per garantire una misurazione coerente dei diritti DII su tutti i sistemi StorageGRID , indipendentemente dalla topologia e dalla configurazione hardware sottostante, Data Infrastructure Insights utilizza la capacità totale disponibile (storagegrid_storage_utilization_total_space_bytes), anziché la capacità RAW basata sul layout del disco fisico.

Per i clienti che utilizzano il modello di licenza basato sulla capacità, StorageGRID viene misurato come storage "Oggetto".

Per i clienti che utilizzano il modello di licenza legacy (MU), StorageGRID viene misurato come storage secondario, a una velocità di 40 TiB per 1 MU.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore NetApp StorageGRID . Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per tale asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
StorageGRID	Magazzinaggio
Nodo	Nodo
Inquilino	Pool di archiviazione
Secchio	Volume interno

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questa origine dati:

- Indirizzo IP host StorageGRID
- Un nome utente e una password per un utente a cui sono stati assegnati i ruoli Metric Query e Tenant Access
- Porta 443 (o 8443 se configurato)

Configurazione

Campo	Descrizione
Indirizzo IP host StorageGRID	Indirizzo IP virtuale di gestione dell'appliance StorageGRID
Nome utente	Nome utilizzato per accedere all'appliance StorageGRID
Password	Password utilizzata per accedere all'appliance StorageGRID

Configurazione avanzata

Campo	Descrizione
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti
Intervallo di sondaggio delle prestazioni (sec)	Il valore predefinito è 900 secondi

Accesso singolo (SSO)

IL"StorageGRID" Le versioni del firmware hanno le corrispondenti versioni API; l'API 3.0 e le versioni più recenti supportano l'accesso Single Sign-On (SSO).

Versione del firmware	Versione API	Supporta l'accesso singolo (SSO)
11,1	2	NO
11,2	3,0	SÌ
11,5	3,3	SÌ

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Nutanix NX

Data Infrastructure Insights utilizza il raccoglitore dati Nutanix per scoprire dati di inventario e prestazioni per i sistemi di archiviazione Nutanix NX.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Nutanix. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Pool di archiviazione	Pool di archiviazione
Contenitore Nutanix	Volume interno
Contenitore Nutanix	Condivisione file
Condivisione NFS	Condividere

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- L'indirizzo IP dei servizi dati esterni per il cluster
- Nome utente e password di sola lettura, a meno che non siano in uso volumi_groups, nel qual caso sono richiesti nome utente e password amministratore
- Requisito porta: HTTPS 443

Configurazione

Campo	Descrizione
Indirizzo IP esterno Prism	L'indirizzo IP dei servizi dati esterni per il cluster
Nome utente	Nome utente per l'account amministratore
Password	Password per l'account amministratore

Configurazione avanzata

Campo	Descrizione
porta TCP	Porta TCP utilizzata per connettersi all'array Nutanix. Il valore predefinito è 9440.
Intervallo di sondaggio dell'inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60 minuti.
Intervallo di sondaggio delle prestazioni (sec)	Intervallo tra i sondaggi sulle prestazioni. Il valore predefinito è 300 secondi.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Oracle ZFS Storage Appliance

Data Infrastructure Insights utilizza il raccoglitore dati Oracle ZFS Storage Appliance per raccogliere dati di inventario e prestazioni.

Terminologia

Data Infrastructure Insights acquisisce informazioni di inventario con il raccoglitore dati Oracle ZFS. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco (SSD)	Disco
Grappolo	Magazzinaggio
Controllore	Nodo di archiviazione
LUN	Volume
Mappa LUN	Mappa del volume
Iniziatore, bersaglio	Maschera del volume
Condividere	Volume interno

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa fonte dati.

Requisiti

- Nomi host per ZFS Controller-1 e ZFS Controller-2
- Nome utente e password dell'amministratore
- Requisito porta: 215 HTTP/HTTPS

Metriche di prestazione richieste

Gli appliance Oracle ZFS offrono agli amministratori di storage un'ampia flessibilità nell'acquisizione di statistiche sulle prestazioni. Data Infrastructure Insights prevede che ogni controller in una coppia ad alta disponibilità sia configurato per acquisire le seguenti metriche:

- smb2.ops[condividi]
- nfs3.ops[condividi]
- nfs4.ops[condividi]
- nfs4-1.ops[condividi]

Se il controller non acquisisce uno o tutti questi dati, probabilmente Data Infrastructure Insights non avrà o segnalerà in modo insufficiente il carico di lavoro sui "Volumi interni".

Configurazione

Campo	Descrizione
Nome host del controller ZFS-1	Nome host per il controller di archiviazione 1
Nome host del controller ZFS-2	Nome host per il controller di archiviazione 2
Nome utente	Nome utente per l'account utente dell'amministratore del sistema di archiviazione
Password	Password per l'account utente amministratore

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS o HTTP, visualizza anche la porta predefinita
Sostituisci porta di connessione	Se vuoto, utilizzare la porta predefinita nel campo Tipo di connessione, altrimenti immettere la porta di connessione da utilizzare
Intervallo di sondaggio dell'inventario	Il valore predefinito è 60 secondi
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 300.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
"Credenziali di accesso non valide"	convalidare l'account utente e la password di Zfs
"Richiesta fallita con stato 404 https://… ..:215/api/access/v1"	Il tuo array ZFS potrebbe essere troppo vecchio per supportare l'API REST. AK 2013.1.3.0 è stata la prima versione del sistema operativo ZFS compatibile con REST API e non tutti gli appliance ZFS possono essere aggiornati a questa versione.
"Errore di configurazione" con messaggio di errore "Il servizio REST è disabilitato"	Verificare che il servizio REST sia abilitato su questo dispositivo.
"Errore di configurazione" con messaggio di errore "Utente non autorizzato per il comando"	Questo errore è probabilmente dovuto al fatto che alcuni ruoli (ad esempio, 'advanced_analytics') non sono inclusi per l'utente configurato. L'applicazione dell'ambito Analytics all'utente con ruolo di sola lettura potrebbe eliminare l'errore. Segui questi passaggi: 1. Nel sistema ZFs, dalla schermata Configurazione → Utenti, sposta il mouse sul ruolo e fai doppio clic per consentire la modifica 2. Selezionare "Analisi" dal menu a discesa Ambito. Viene visualizzato un elenco delle possibili proprietà. 3. Fare clic sulla casella di controllo più in alto per selezionare tutte e tre le proprietà. 4. Fare clic sul pulsante Aggiungi sul lato destro. 5. Fare clic sul pulsante Applica in alto a destra della finestra pop-up. La finestra pop-up si chiuderà.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati Pure Storage FlashArray

Data Infrastructure Insights utilizza il raccoglitore dati Pure Storage FlashArray per raccogliere dati di inventario e prestazioni.

Terminologia

Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per la risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Unità (SSD)	Disco

Termine del fornitore/modello	Termine Data Infrastructure Insights
Vettore	Magazzinaggio
Controllore	Nodo di archiviazione
Volume	Volume
Mappa LUN	Mappa del volume
Iniziatore, bersaglio	Maschera del volume

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Indirizzo IP del sistema di archiviazione
- Nome utente e password per l'account Amministratore del sistema di archiviazione Pure.
- Requisito porta: HTTP/HTTPS 80/443

Configurazione

Campo	Descrizione
Indirizzo IP host FlashArray	Indirizzo IP del sistema di archiviazione
Nome utente	Nome utente con privilegi di amministratore
Password per l'account con privilegi di amministratore	Password

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	Scegli HTTP o HTTPS. Visualizza anche la porta predefinita.
Sostituisci la porta TCP	Se vuoto, utilizzare la porta predefinita nel campo Tipo di connessione, altrimenti immettere la porta di connessione da utilizzare
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60 minuti
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 300

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
"Credenziali di accesso non valide" con messaggi di errore "La policy non consente" o "Non sei autorizzato"	Convalida l'account utente e la password Pure tramite l'interfaccia http Pure

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati di Red Hat Virtualization

Data Infrastructure Insights utilizza il raccoglitore dati Red Hat Virtualization per raccogliere dati di inventario dai carichi di lavoro virtualizzati Linux e Microsoft Windows.

Terminologia

Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per la risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco	Disco virtuale
Ospite	Ospite
Macchina virtuale	Macchina virtuale
Dominio di archiviazione	Archivio dati
Unità logica	LUN

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

- Indirizzo IP del server RHEV sulla porta 443 tramite REST API
- Nome utente e password di sola lettura
- RHEV versione 3.0+

Configurazione

Campo	Descrizione
Indirizzo IP del server RHEV	Indirizzo IP del sistema di archiviazione
Nome utente	Nome utente con privilegi di amministratore
Password per l'account con privilegi di amministratore	Password

Configurazione avanzata

Campo	Descrizione
Porta di comunicazione HTTPS	Porta utilizzata per la comunicazione HTTPS con RHEV
Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 20 minuti.

Risoluzione dei problemi

Ulteriori informazioni su questo Data Collector possono essere trovate da"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Raccoglitore dati CDM Rubrik

Data Infrastructure Insights utilizza il raccoglitore dati Rubrik per acquisire dati di inventario e prestazioni dagli storage appliance Rubrik.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati Rubrik. Per ogni tipo di risorsa acquisita da Data Infrastructure Insights, viene mostrata la terminologia più comune utilizzata per tale risorsa. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Grappolo	Deposito, piscina di stoccaggio
Nodo	Nodo di archiviazione
Disco	Disco

Nota: queste sono solo mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa fonte dati.

Requisiti

Per configurare questo raccoglitore dati sono necessari i seguenti elementi:

- L'unità di acquisizione Data Infrastructure Insights avvierà le connessioni alla porta TCP 443 al cluster Rubrik. Un collettore per cluster.
- Indirizzo IP del cluster Rubrik.
- Nome utente e password per il cluster.
- Indirizzo IP o nome host del cluster Rubrik.
- Per l'autenticazione di base, un nome utente e una password per il cluster. Se preferisci utilizzare l'autenticazione basata sull'account di servizio, hai bisogno di un account di servizio, di un segreto e di un ID organizzazione
- Requisito porta: HTTPS 443

Configurazione

Campo	Descrizione
Proprietà intellettuale	Indirizzo IP del cluster Rubrik
Nome utente / Account di servizio	Nome utente per il cluster
Password / Segreto	Password per il cluster

Campo	Descrizione
ID organizzazione per l'account di servizio	Deve essere la stringa completa, ad esempio "Organization:::nnnnnn-nnnn….."

Configurazione avanzata

Intervallo di sondaggio dell'inventario (min)	Il valore predefinito è 60
Intervallo di sondaggio sulle prestazioni (sec)	Il valore predefinito è 300

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Ho ricevuto un messaggio che indica che è stato creato più di uno spazio di archiviazione.	Verificare che il cluster sia configurato correttamente e che il collettore punti a un singolo cluster.
Il sondaggio fallisce con 400 [Richiesta non valida]…. ManagedId non valido….	Hai popolato il campo ID organizzazione con un valore, ma il cluster Rubrik NON ritiene che si tratti di un ID organizzazione valido, nonostante il messaggio di errore di Rubrik lo chiami "ManagedId"

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Configurazione del raccoglitore dati VMware VSphere

Il data collector per VMware vSphere raccoglie informazioni sulle prestazioni e sulla configurazione delle VM guest e degli host ESXi e richiede privilegi di sola lettura su tutti gli oggetti all'interno di vSphere. A partire da agosto 2024, vSphere Collector importa anche i messaggi di registro dagli ambienti vSphere e alcune metriche specifiche di VMware. Si prega di notare che Data Infrastructure Insights può recuperare informazioni sui registri VMware solo da ambienti vSphere 8.0.1 o versioni successive. Allo stesso modo, le metriche specifiche del fornitore sono supportate solo per gli ambienti vSphere 7+. Pertanto, potrebbe essere opportuno disattivare la casella di controllo dei registri e/o delle metriche specifiche del fornitore su un determinato raccoglitore se punta a un'istanza vSphere precedente.

Terminologia

Data Infrastructure Insights acquisisce le seguenti informazioni di inventario dal raccoglitore dati VMware vSphere. Per ogni tipologia di asset acquisito viene mostrata la terminologia più comune utilizzata per l'asset. Quando si visualizza o si risolve un problema con questo strumento di raccolta dati, tenere presente la seguente terminologia:

Termine del fornitore/modello	Termine Data Infrastructure Insights
Disco virtuale	Disco
Ospite	Ospite
Macchina virtuale	Macchina virtuale
Archivio dati	Archivio dati
LUN	Volume
Porta Fibre Channel	Porta

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo raccoglitore di dati.

Requisiti

Per configurare questo raccoglitore dati sono necessarie le seguenti informazioni:

- Indirizzo IP del server Virtual Center
- Nome utente e password di sola lettura nel Virtual Center
- Richiediamo privilegi di sola lettura su tutti gli oggetti all'interno di Virtual Center.
- Accesso SDK sul server Virtual Center, solitamente già configurato.
- Requisiti della porta: http-80 https-443
- Convalida l'accesso:
  - Accedi al Virtual Center Client utilizzando il nome utente e la password sopra indicati
  - Verifica SDK abilitato: telnet <vc_ip> 443

Installazione e connessione

Campo	Descrizione
Nome	Nome univoco per il raccoglitore di dati
Unità di acquisizione	Nome dell'unità di acquisizione

Configurazione

Campo	Descrizione
Indirizzo IP del centro virtuale	Indirizzo IP del Centro Virtuale
Nome utente	Nome utente utilizzato per accedere al Centro Virtuale
Password	Password utilizzata per accedere al Centro Virtuale

Configurazione avanzata

Nella schermata di configurazione avanzata, seleziona la casella **Prestazioni VM** per raccogliere i dati sulle prestazioni. La raccolta dell'inventario è abilitata per impostazione predefinita. È possibile configurare i seguenti campi:

Campo	Descrizione
Intervallo di sondaggio dell’inventario (min)	Il valore predefinito è 20
Filtra le VM	Seleziona CLUSTER, DATACENTER o ESX HOST
Scegli "Escludi" o "Includi" per specificare un elenco	Creare un elenco di filtri (CLUSTER, DATACENTER e/o ESX_HOST)
Numero di tentativi	Il valore predefinito è 3
Porta di comunicazione	Il valore predefinito è 443
Filtra elenco dispositivi…	Questo elenco deve essere composto da corrispondenze esatte di stringhe: se si intende filtrare per ESX_HOST, è necessario creare un elenco delimitato da virgole dei "nomi" esatti degli host ESX, come riportato sia in Data Infrastructure Insights che in vSphere. Questi "nomi" possono essere indirizzi IP, semplici nomi host o nomi di dominio completi (FQDN): ciò è determinato dal nome assegnato a questi host quando sono stati aggiunti originariamente a vSphere. Quando si filtra per CLUSTER, utilizzare i nomi dei cluster in stile Data Infrastructure Insights come riportati da CI sugli hypervisor. Data Infrastructure Insights antepone al nome del cluster vSphere il nome del data center vSphere e una barra. "DC1/clusterA" è il nome del cluster che Data Infrastructure Insights riporterebbe su un hypervisor nel clusterA all’interno del data center DC1.
Intervallo di sondaggio delle prestazioni (sec)	Il valore predefinito è 300

Mappatura dei tag VMware alle annotazioni Data Infrastructure Insights

Il raccoglitore dati VMware consente di popolare le annotazioni di Data Infrastructure Insights con tag configurati su VMware. Il nome dell’annotazione DII deve essere identico al nome della **categoria** VMware; il tag viene quindi applicato come valore di annotazione di un’annotazione DII con lo stesso nome della categoria. Data Infrastructure Insights popolerà sempre le annotazioni di tipo testo con lo stesso nome e farà un "miglior tentativo" per popolare le annotazioni di altri tipi (numero, valore booleano, ecc.). Se l’annotazione è di un tipo diverso e il raccoglitore dati non riesce a popolarla, potrebbe essere necessario rimuovere l’annotazione e ricrearla come tipo di testo.

Si noti che i tag VMware potrebbero fare distinzione tra maiuscole e minuscole, mentre i tag Data Infrastructure Insights non fanno distinzione tra maiuscole e minuscole. Quindi, se si crea un’annotazione denominata "OWNER" in Data Infrastructure Insights e tag denominati "OWNER", "Owner" e "owner" in VMware, tutte queste varianti di "owner" verrebbero mappate all’annotazione "OWNER" di Cloud Insight.

Tieni presente quanto segue:

- Attualmente Data Infrastructure Insights pubblica automaticamente solo le informazioni di supporto per i dispositivi NetApp .
- Poiché queste informazioni di supporto sono conservate in formato annotazione, è possibile interrogarle o utilizzarle nelle dashboard.
- Se un utente sovrascrive o svuota il valore dell’annotazione, il valore viene nuovamente compilato automaticamente quando Data Infrastructure Insights aggiorna le annotazioni, operazione che avviene una

volta al giorno.

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi con questo strumento di raccolta dati:

Inventario

Problema:	Prova questo:
Errore: l'elenco da includere per filtrare le VM non può essere vuoto	Se è selezionato Includi elenco, elenca i nomi validi di DataCenter, Cluster o Host per filtrare le VM
Errore: impossibile creare una connessione a VirtualCenter all'IP	Possibili soluzioni: * Verificare le credenziali e l'indirizzo IP immessi. * Provare a comunicare con Virtual Center utilizzando VMware Infrastructure Client. * Prova a comunicare con Virtual Center utilizzando Managed Object Browser (ad esempio MOB).
Errore: VirtualCenter su IP ha un certificato non conforme richiesto da JVM	Soluzioni possibili: * Consigliato: rigenerare il certificato per Virtual Center utilizzando una chiave RSA più potente (ad esempio a 1024 bit). * Sconsigliato: modificare la configurazione java.security della JVM per sfruttare il vincolo jdk.certpath.disabledAlgorithms per consentire la chiave RSA a 512 bit. Vedere "Note di rilascio dell'aggiornamento 40 di JDK 7" .
Vedo il messaggio: "Il pacchetto VMware Logs non è supportato su VMware con versione precedente alla 8.0.1"	La raccolta dei log non è supportata nelle versioni di VMware precedenti alla 8.0.1. Aggiorna l'infrastruttura del VI Center alla versione 8.0.1 o successiva se desideri utilizzare la funzionalità Raccolte di log in Data Infrastructure Insights. Per maggiori informazioni, vedere questo"Articolo della Knowledge Base" .

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Riferimento al Data Collector - Servizi

Raccolta dati nodo

Data Infrastructure Insights raccoglie le metriche dal nodo su cui installi un agente.

Installazione

1. Da **Observability > Collectors**, seleziona un sistema operativo/piattaforma. Si noti che l'installazione di qualsiasi raccoglitore di dati di integrazione (Kubernetes, Docker, Apache, ecc.) configurerà anche la raccolta di dati del nodo.
2. Seguire le istruzioni per configurare l'agente. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

Oggetti e contatori

I seguenti oggetti e i relativi contatori vengono raccolti come metriche Node:

Oggetto:	Identificatori:	Attributi:	Punti dati:
File system del nodo	Tipo di percorso del dispositivo UUID del nodo	IP del nodo Nome del nodo Modalità del sistema operativo del nodo	Inode liberi Inode liberi Totale inode utilizzati Totale utilizzato Totale utilizzato
Nodo Disco	Disco UUID del nodo	IP del nodo Nome del nodo Sistema operativo del nodo	Tempo di I/O Totale IOPS in corso Byte letti (al sec) Tempo di lettura Letture totali (al sec) Tempo di I/O ponderato Byte scritti totali (al sec) Tempo di scrittura Scritture totali (al sec) Lunghezza coda disco corrente Tempo di scrittura Tempo di lettura Tempo di I/O
Nodo CPU	CPU UUID del nodo	IP del nodo Nome del nodo Sistema operativo del nodo	Utilizzo CPU di sistema Utilizzo CPU utente Utilizzo CPU inattiva Utilizzo CPU processore Utilizzo CPU interrupt Utilizzo CPU DPC

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo	Nodo UUID	IP del nodo Nome del nodo Sistema operativo del nodo	Tempo di avvio del kernel Commutazioni di contesto del kernel (al secondo) Entropia del kernel disponibile Interrupt del kernel (al secondo) Processi del kernel forkati (al secondo) Memoria attiva Memoria disponibile Memoria totale disponibile Memoria bufferizzata Memoria memorizzata nella cache Limite di commit Memoria memorizzata come memoria Memoria sporca Memoria libera alta Memoria libera alta Memoria totale Memoria di dimensioni di pagina enormi Pagine enormi Memoria libera Pagine enormi Memoria totale bassa Memoria libera bassa Memoria totale Memoria mappata Tabelle delle pagine Memoria Memoria condivisa Memoria slab Swap di memoria nella cache Swap di memoria libera Swap di memoria totale Memoria totale utilizzata Memoria totale utilizzata Memoria Vmalloc Chunk Memory Vmalloc Memoria totale Vmalloc utilizzata Memoria cablata Writeback di memoria Writeback di memoria totale Memoria temporanea Errori della cache di memoria Richiesta di memoria Zero errori Errori di pagina di memoria Pagine di memoria Memoria non di paging Memoria di paging Memoria core della cache Cache di standby Memoria normale Cache di standby di riserva Errori di transizione di memoria Processi Processi bloccati Processi morti Processi

Oggetto:	Identificatori:	Attributi:	Punti dati:
Rete di nodi	UUID del nodo dell'interfaccia di rete	Nome nodo IP nodo Sistema operativo nodo	Byte ricevuti Byte inviati Pacchetti in uscita Pacchetti scartati Pacchetti in uscita Errori Pacchetti ricevuti Pacchetti scartati Pacchetti ricevuti Errori Pacchetti ricevuti Pacchetti inviati

Impostare

Le informazioni sulla configurazione e sulla risoluzione dei problemi sono disponibili su"Configurazione di un agente" pagina.

Raccoglitore dati ActiveMQ

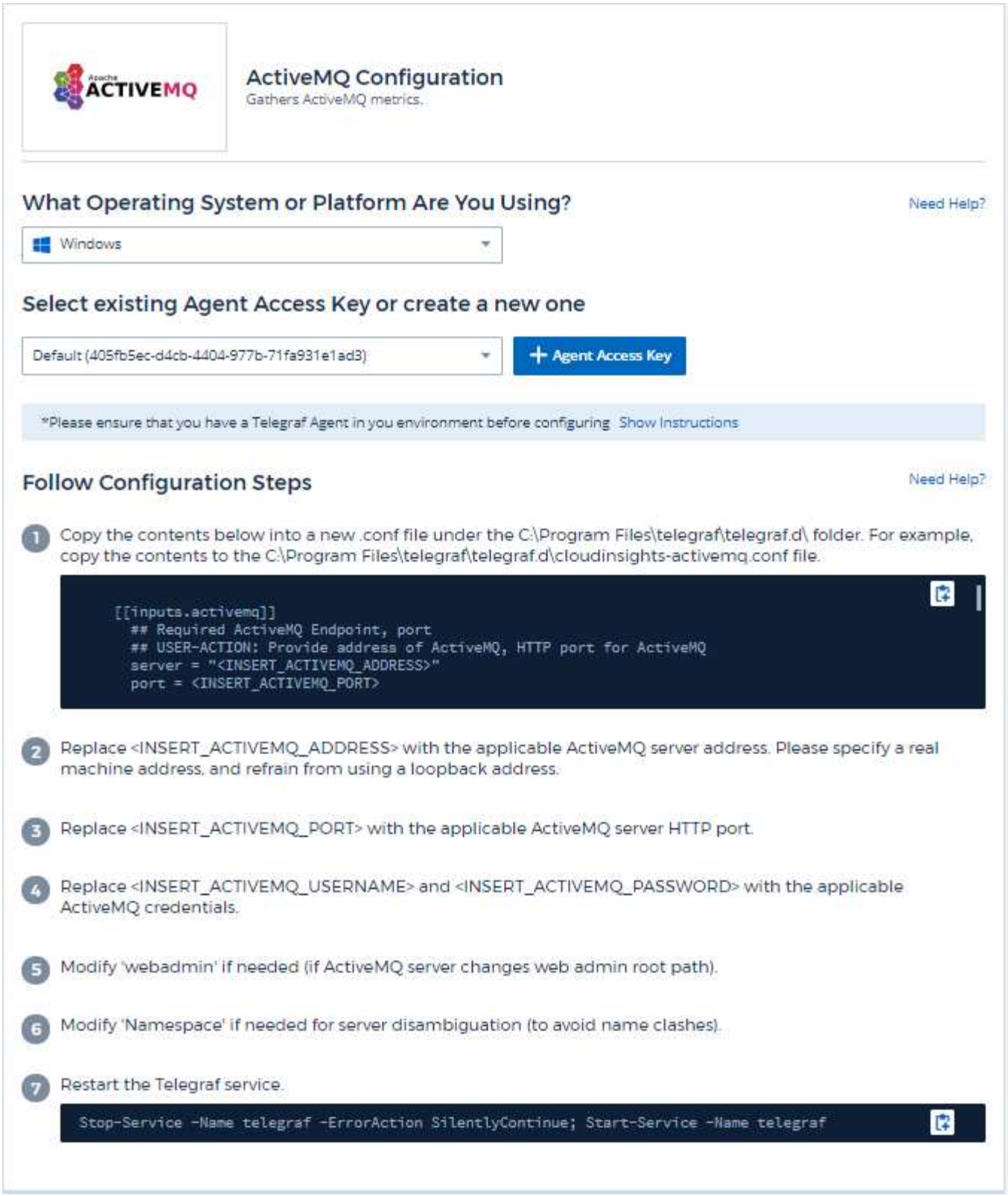
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da ActiveMQ.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli ActiveMQ.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel "Documentazione ActiveMQ"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Coda ActiveMQ	Server porta coda spazio dei nomi	Nome nodo IP nodo UUID nodo	Conteggio consumatori Conteggio de-accodamento Conteggio accodamento Dimensione coda
Abbonato ActiveMQ	ID client ID connessione Porta Spazio dei nomi del server	È attivo Nome nodo di destinazione IP nodo UUID nodo Selettore sistema operativo nodo Sottoscrizione	Conteggio dei dequeue Conteggio dei dispatched Dimensione coda inviata Conteggio dei enqueue Dimensione coda in sospeso
Argomento ActiveMQ	Spazio dei nomi del server della porta dell'argomento	Nome nodo IP nodo UUID nodo Sistema operativo nodo	Conteggio consumatori Conteggio de-accodamento Conteggio accodamento Dimensione

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Apache Data Collector

Questo raccoglitore di dati consente la raccolta di dati dai server Apache sul tuo tenant.

Prerequisiti

- Devi avere il tuo server Apache HTTP configurato e funzionante correttamente
- Devi avere i permessi sudo o amministratore sul tuo host agente/VM
- In genere, il modulo Apache *mod_status* è configurato per esporre una pagina nella posizione '/server-status?auto' del server Apache. Per raccogliere tutti i campi disponibili, è necessario abilitare l'opzione *ExtendedStatus*. Per informazioni su come configurare il server, consultare la documentazione del modulo Apache: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

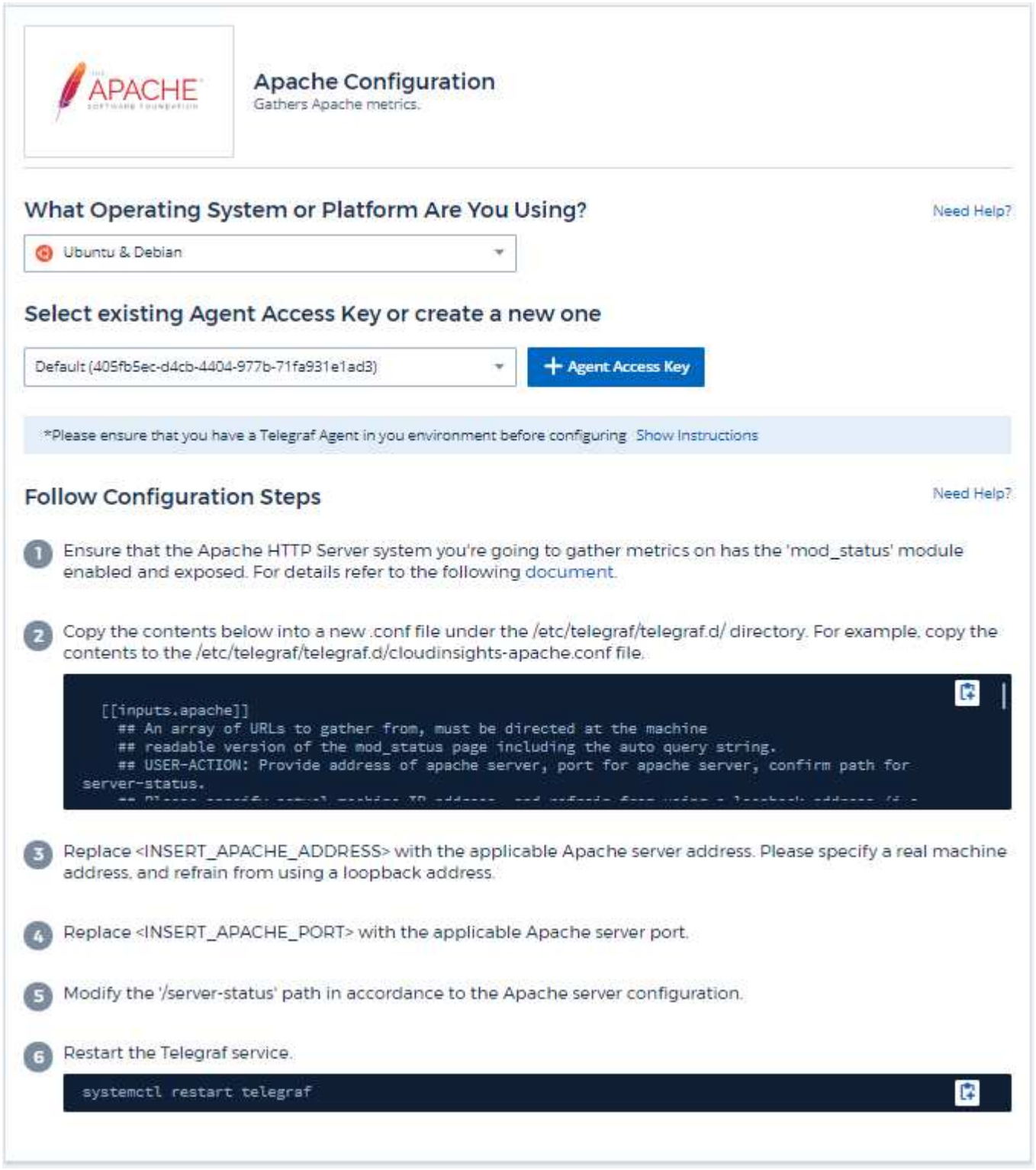
Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Apache.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.

4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Il plugin di Telegraf per il server HTTP di Apache si basa sull'abilitazione del modulo 'mod_status'. Se questa opzione è abilitata, il server HTTP di Apache esporrà un endpoint HTML che può essere visualizzato sul browser o recuperato per l'estrazione dello stato di tutta la configurazione del server HTTP di Apache.

Compatibilità:

La configurazione è stata sviluppata per la versione 2.4.38 del server HTTP di Apache.

Abilitazione di mod_status:

L'abilitazione e l'esposizione dei moduli 'mod_status' comporta due passaggi:

- Modulo di abilitazione
- Esposizione delle statistiche dal modulo

Modulo di abilitazione:

Il caricamento dei moduli è controllato dal file di configurazione in '/usr/local/apache/conf/httpd.conf'. Modifica il file di configurazione e rimuovi il commento dalle seguenti righe:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Visualizzazione delle statistiche dal modulo:

L'esposizione di 'mod_status' è controllata dal file di configurazione in '/usr/local/apache2/conf/extra/httpd-info.conf'. Assicuratevi di avere quanto segue nel file di configurazione (almeno, ci saranno altre direttive):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Per istruzioni dettagliate sul modulo 'mod_status', vedere"Documentazione di Apache"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Apache	Server dello spazio dei nomi	IP del nodo Nome del nodo Porta Generazione della configurazione del server padre Generazione MPM del server padre Il tempo di attività del server si sta interrompendo	Lavoratori occupati Byte per richiesta Byte al secondo CPU CPU di sistema figli CPU utente figli Carico CPU di sistema CPU utente Connessioni asincrone Chiusura Connessioni asincrone Keep Alive Connessioni asincrone Scrittura Connessioni Durata totale per richiesta Lavoratori inattivi Carico medio (ultimo minuto) Carico medio (ultimi 15 minuti) Carico medio (ultimi 5 minuti) Processi Richieste al secondo Accessi totali Durata totale Kbyte totali Tabellone segnapunti Chiusura tabellone segnapunti Ricerche DNS Tabellone segnapunti Completamento tabellone segnapunti Pulizia inattiva tabellone segnapunti Keep Alive Registrazione tabellone segnapunti Apertura tabellone segnapunti Lettura tabellone segnapunti Invio tabellone segnapunti Avvio tabellone segnapunti In attesa

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Consul Data Collector

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Consul.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Console.

   Se non hai configurato un agente per la raccolta, ti verrà richiesto di"installare un agente" sul tuo inquilino.

   Se hai già configurato un agente, seleziona il sistema operativo o la piattaforma appropriati e fai clic su

Continua.

2. Seguire le istruzioni nella schermata Configurazione del Consul per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

Impostare

Le informazioni possono essere trovate nel"Documentazione del console" .

Oggetti e contatori per console

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Console	Nodo del servizio ID di controllo dello spazio dei nomi	IP del nodo Sistema operativo del nodo UUID del nodo Nome del nodo Nome del servizio Controlla nome ID del servizio Stato	Avviso di sorpasso critico

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Couchbase Data Collector

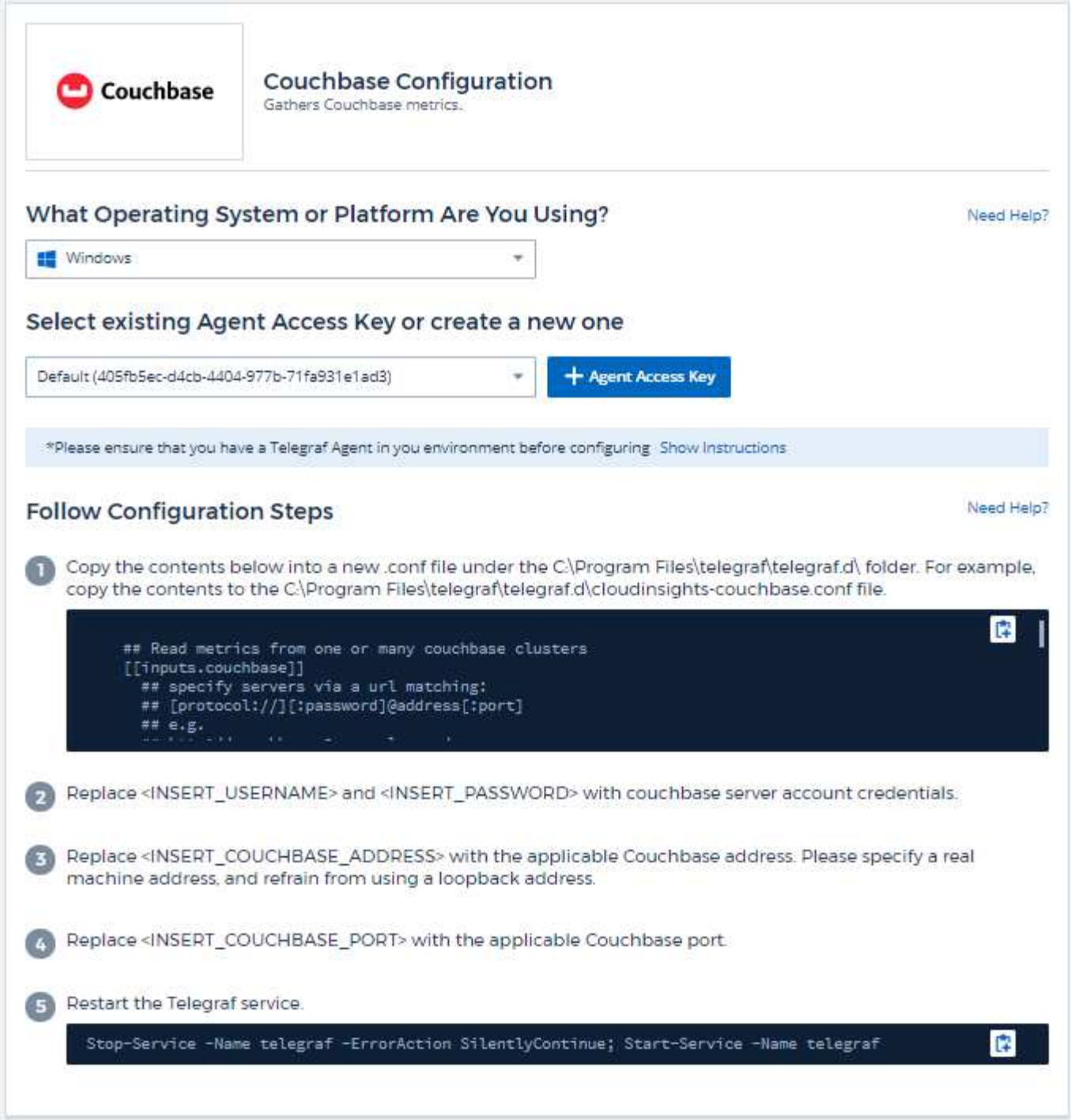
Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Couchbase.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Couchbase.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione di Couchbase" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo Couchbase	Nome host del nodo Couchbase del cluster dello spazio dei nomi	Nome nodo IP nodo	Memoria libera Memoria totale
Secchio Couchbase	Cluster di bucket dello spazio dei nomi	Nome nodo IP nodo	Dati utilizzati Recuperi dati Disco utilizzato Numero di elementi Memoria utilizzata Operazioni al secondo Quota utilizzata

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

CouchDB Data Collector

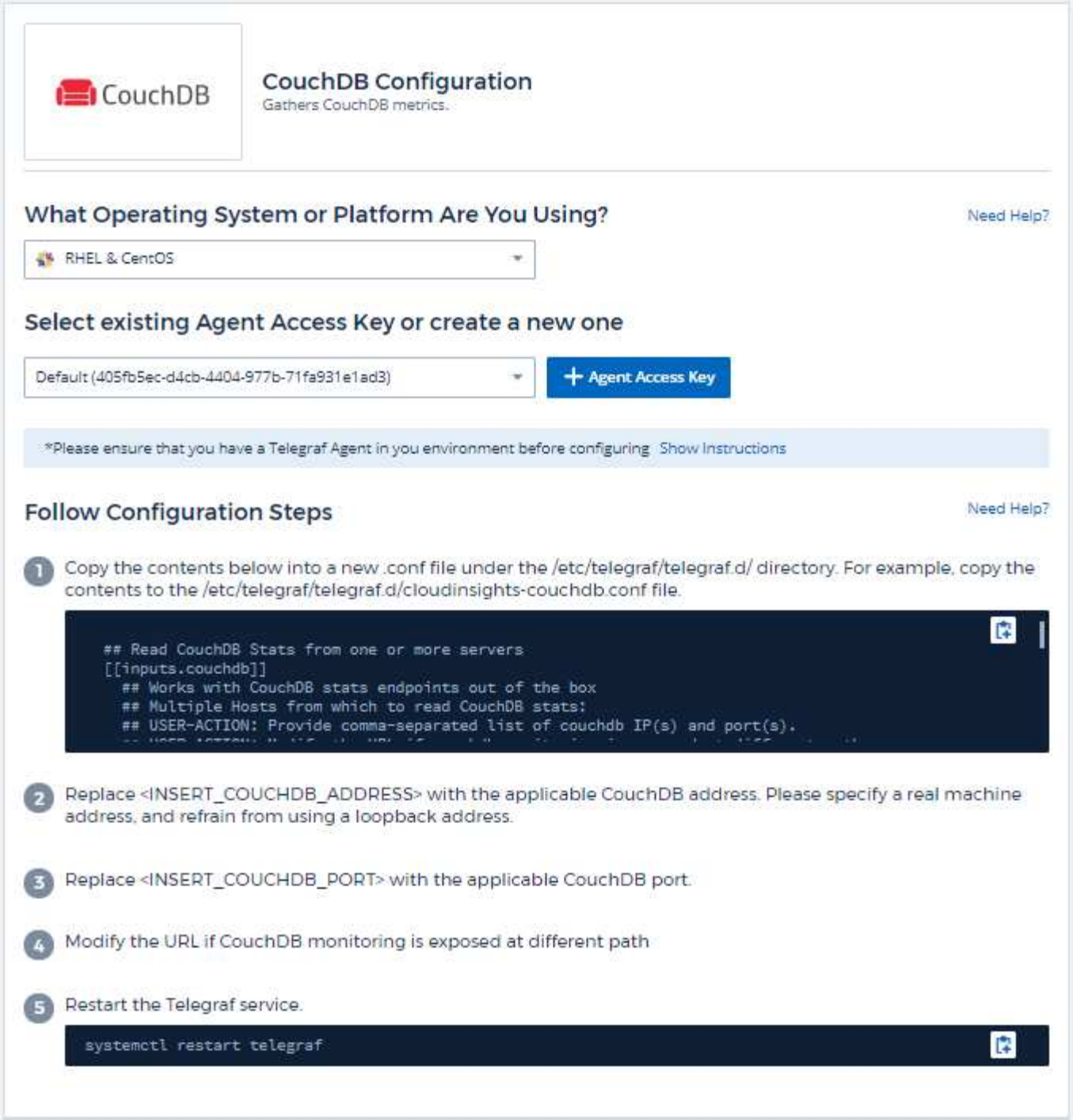
Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da CouchDB.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli CouchDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione di CouchDB" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
CouchDB	Server dello spazio dei nomi	Nome nodo IP nodo	Hit della cache di autenticazione Miss della cache di autenticazione Letture del database Scritture del database Database aperti File del sistema operativo aperti Tempo massimo di richiesta Tempo minimo di richiesta Metodi di richiesta HTTPD Copia Metodi di richiesta HTTPD Elimina Metodi di richiesta HTTPD Ottieni Metodi di richiesta HTTPD Intestazione Metodi di richiesta HTTPD Post Metodi di richiesta HTTPD Inserisci Codici di stato 200 Codici di stato 201 Codici di stato 202 Codici di stato 301 Codici di stato 304 Codici di stato 400 Codici di stato 401 Codici di stato 403 Codici di stato 404 Codici di stato 405 Codici di stato 409 Codici di stato 412 Codici di stato 500

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Docker Data Collector

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Docker.

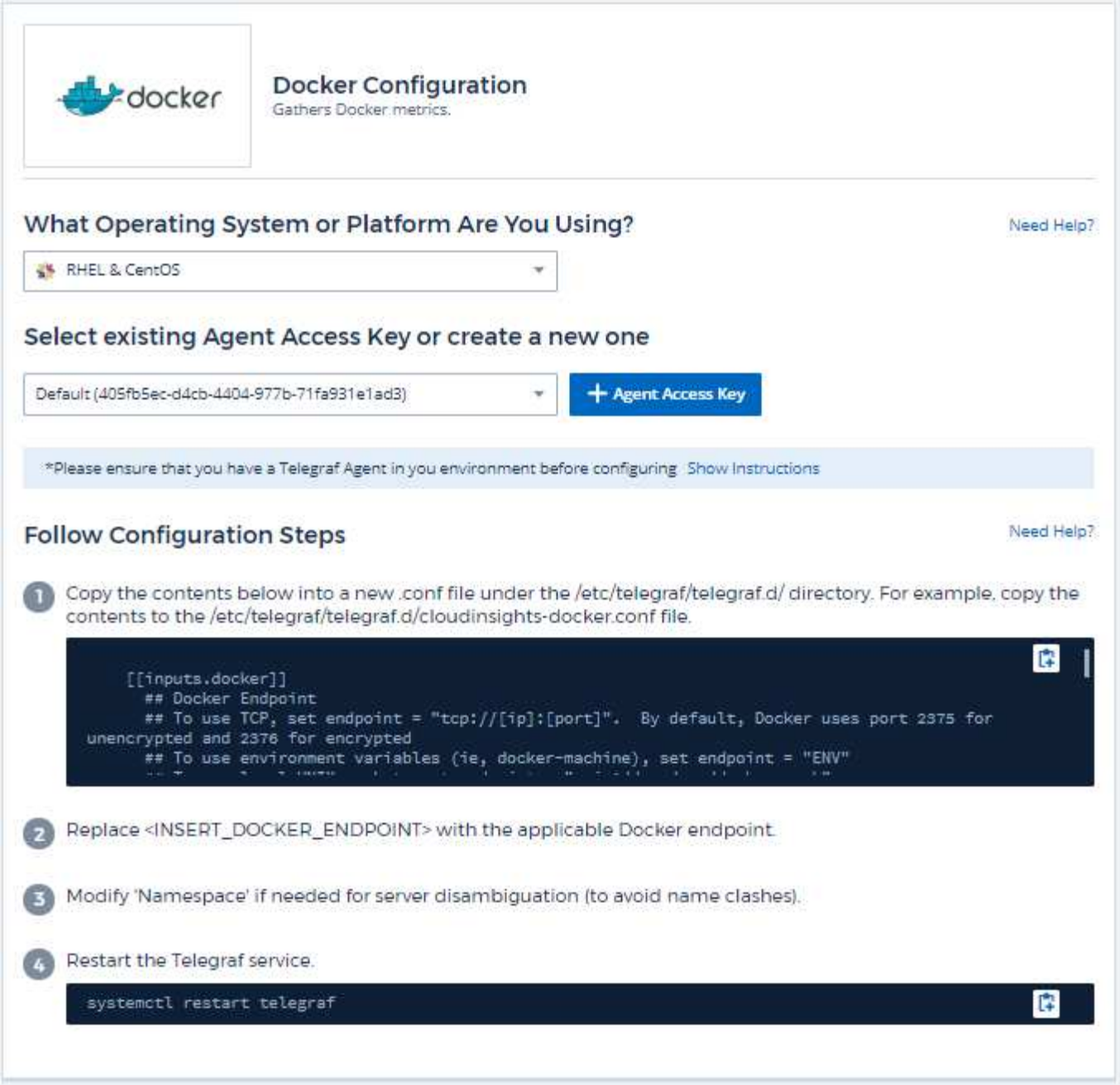
Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Docker.

   Se non hai configurato un agente per la raccolta, ti verrà richiesto di"installare un agente" sul tuo inquilino.

   Se hai già configurato un agente, seleziona il sistema operativo o la piattaforma appropriati e fai clic su **Continua**.

2. Seguire le istruzioni nella schermata Configurazione Docker per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Il plugin di input Telegraf per Docker raccoglie le metriche tramite un socket UNIX specificato o un endpoint TCP.

Compatibilità

La configurazione è stata sviluppata per Docker versione 1.12.6.

Impostazione

Accesso a Docker tramite un socket UNIX

Se l'agente Telegraf è in esecuzione su baremetal, aggiungere l'utente Unix Telegraf al gruppo Unix Docker eseguendo quanto segue:

```
 sudo usermod -aG docker telegraf
Se l'agente Telegraf è in esecuzione all'interno di un pod Kubernetes,
esporre il socket Docker Unix mappando il socket nel pod come volume e
quindi montando tale volume su /var/run/docker.sock.  Ad esempio, aggiungi
quanto segue al PodSpec:
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Quindi, aggiungi quanto segue al contenitore:

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Si noti che il programma di installazione Data Infrastructure Insights fornito per la piattaforma Kubernetes si occupa automaticamente di questa mappatura.

Accedi a Docker tramite un endpoint TCP

Per impostazione predefinita, Docker utilizza la porta 2375 per l'accesso non crittografato e la porta 2376 per l'accesso crittografato.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Motore Docker	Motore Docker dello spazio dei nomi	Nome nodo IP nodo UUID nodo Sistema operativo nodo Cluster Kubernetes Versione Docker Unità	Contenitori di memoria Contenitori Contenitori in pausa Contenitori in esecuzione CPU arrestate Routine di avvio Immagini Eventi di ascolto Descrittori di file utilizzati Dati Dati disponibili Dati totali utilizzati Metadati Metadati disponibili Metadati totali utilizzati Dimensione blocco pool

Oggetto:	Identificatori:	Attributi:	Punti dati:
Contenitore Docker	Nome del contenitore dello spazio dei nomi Docker Engine	Hash del contenitore Kubernetes Porte del contenitore Kubernetes Conteggio riavvii del contenitore Kubernetes Percorso del messaggio di terminazione del contenitore Kubernetes Criterio del messaggio di terminazione del contenitore Kubernetes Periodo di grazia per la terminazione del pod Kubernetes Immagine del contenitore Stato del contenitore Versione del contenitore Nome del nodo Percorso del registro del contenitore Kubernetes Nome del contenitore Kubernetes Tipo di Docker Kubernetes Nome del pod Kubernetes Spazio dei nomi del pod Kubernetes UID del pod Kubernetes ID sandbox Kubernetes IP del nodo UUID del nodo Versione Docker Configurazione IO Kubernetes visualizzata Sorgente della configurazione IO Kubernetes SCC IO OpenShift Descrizione Kubernetes Nome visualizzato Kubernetes Tag OpenShift Kompose Service Pod Template Hash Controller Revisione Hash Generazione del modello del pod Licenza Schema Data di build Schema Licenza Nome schema URL schema URL VCS schema Fornitore schema Versione schema Schema Versione schema Manutentore Pod cliente Kubernetes StatefulSet Nome pod Tenant Webconsole Architettura URL origine autorevole Data di build Host build RH Componente RH	Memoria attiva Memoria anonima Memoria attiva Memoria file cache Limite gerarchico della memoria Memoria inattiva Memoria anonima Memoria inattiva Limite di memoria file Memoria file mappata Utilizzo massimo della memoria Errore di pagina della memoria Errore di pagina maggiore della memoria Memoria paginata in memoria paginata in memoria paginata in memoria Dimensione del set residente della memoria Dimensione del set residente della memoria Enorme Memoria totale attiva Memoria anonima Memoria file attiva Memoria cache totale Memoria anonima Memoria file inattiva Memoria file mappata Memoria totale Errore di pagina maggiore della memoria Totale Memoria paginata in memoria totale Paginata in memoria totale Paginata in memoria totale Dimensione del set residente della memoria Totale Dimensione del set residente della memoria Enorme Memoria totale non rimuovibile Utilizzo della memoria non rimuovibile Percentuale di utilizzo della memoria Codice di uscita OOM PID eliminato Avviato con sequenza di errori

Oggetto:	Identificatori:	Attributi:	Punti dati:
Docker Container Block IO	Namespace Contenitore Nome Dispositivo Motore Docker	Hash del contenitore Kubernetes Porte del contenitore Kubernetes Conteggio riavvii del contenitore Kubernetes Percorso del messaggio di terminazione del contenitore Kubernetes Criterio del messaggio di terminazione del contenitore Kubernetes Periodo di grazia per la terminazione del pod Kubernetes Immagine del contenitore Stato del contenitore Versione del contenitore Nome del nodo Percorso del registro del contenitore Kubernetes Nome del contenitore Kubernetes Tipo di Docker Kubernetes Nome del pod Kubernetes Spazio dei nomi del pod Kubernetes UID del pod Kubernetes ID sandbox Kubernetes IP del nodo UUID del nodo Versione Docker Configurazione Kubernetes visualizzata Sorgente della configurazione Kubernetes OpenShift SCC Descrizione di Kubernetes Nome visualizzato di Kubernetes Tag di OpenShift Schema Versione dello schema Hash del modello del pod Hash di revisione del controller Generazione del modello del pod Servizio Kompose Data di build dello schema Licenza dello schema Nome dello schema Fornitore dello schema Pod del cliente Nome del pod StatefulSet di Kubernetes Tenant Webconsole Data di build Fornitore della licenza Architettura URL sorgente autorevole Host di build RH Componente RH Ambito di distribuzione	Byte del servizio IO ricorsivi asincroni Byte del servizio IO ricorsivi in lettura Byte del servizio IO ricorsivi in sincronizzazione Byte del servizio IO ricorsivi totali Byte del servizio IO ricorsivi in scrittura Byte del servizio IO ricorsivi in asincroni serviti in lettura ricorsiva Byte del servizio IO ricorsivi in sincronizzazione serviti in lettura ricorsiva Byte del servizio IO ricorsivi totali serviti in scrittura ricorsiva

Oggetto:	Identificatori:	Attributi:	Punti dati:
Rete di contenitori Docker	Namespace Container Nome Rete Docker Engine	Immagine del contenitore Stato del contenitore Versione del contenitore Nome del nodo IP del nodo UUID del nodo Sistema operativo del nodo Cluster K8s Versione Docker ID del contenitore	RX eliminati Byte RX Errori RX Pacchetti RX TX eliminati Byte TX Errori TX Pacchetti TX

Oggetto:	Identificatori:	Attributi:	Punti dati:
CPU del contenitore Docker	Nome del contenitore dello spazio dei nomi CPU Motore Docker	Hash del contenitore Kubernetes Porte del contenitore Kubernetes Conteggio riavvii del contenitore Kubernetes Percorso del messaggio di terminazione del contenitore Kubernetes Criterio del messaggio di terminazione del contenitore Kubernetes Periodo di grazia per la terminazione del pod Kubernetes Configurazione Kubernetes visualizzata Origine della configurazione Kubernetes Immagine del contenitore OpenShift SCC Stato del contenitore Versione del contenitore Nome del nodo Percorso del registro del contenitore Kubernetes Nome del contenitore Kubernetes Tipo di Docker Kubernetes Nome del pod Kubernetes Spazio dei nomi del pod Kubernetes UID del pod Kubernetes ID sandbox Kubernetes IP del nodo UUID del nodo Sistema operativo del nodo Versione Docker del cluster Kubernetes Descrizione di Kubernetes Nome visualizzato di Kubernetes Tag OpenShift Versione dello schema Hash del modello del pod Hash di revisione del controller Generazione del modello del pod Servizio Kompose Data di build dello schema Licenza dello schema Nome dello schema Fornitore dello schema Pod del cliente Nome del pod StatefulSet Kubernetes Tenant Webconsole Data di build Fornitore della licenza Architettura URL sorgente autorevole Host di build	Periodi di limitazione Periodi di limitazione della limitazione Tempo di limitazione della limitazione Utilizzo in modalità kernel Utilizzo in modalità utente Percentuale di utilizzo Utilizzo del sistema Utilizzo totale

Risoluzione dei problemi

Problema:	Prova questo:
Dopo aver seguito le istruzioni nella pagina di configurazione, non vedo le mie metriche Docker in Data Infrastructure Insights .	Controllare i registri dell'agente Telegraf per vedere se segnala il seguente errore: E! Errore nel plugin [inputs.docker]: Autorizzazione negata durante il tentativo di connessione al socket del demone Docker. In tal caso, adottare le misure necessarie per consentire all'agente Telegraf di accedere al socket Unix Docker come specificato sopra.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

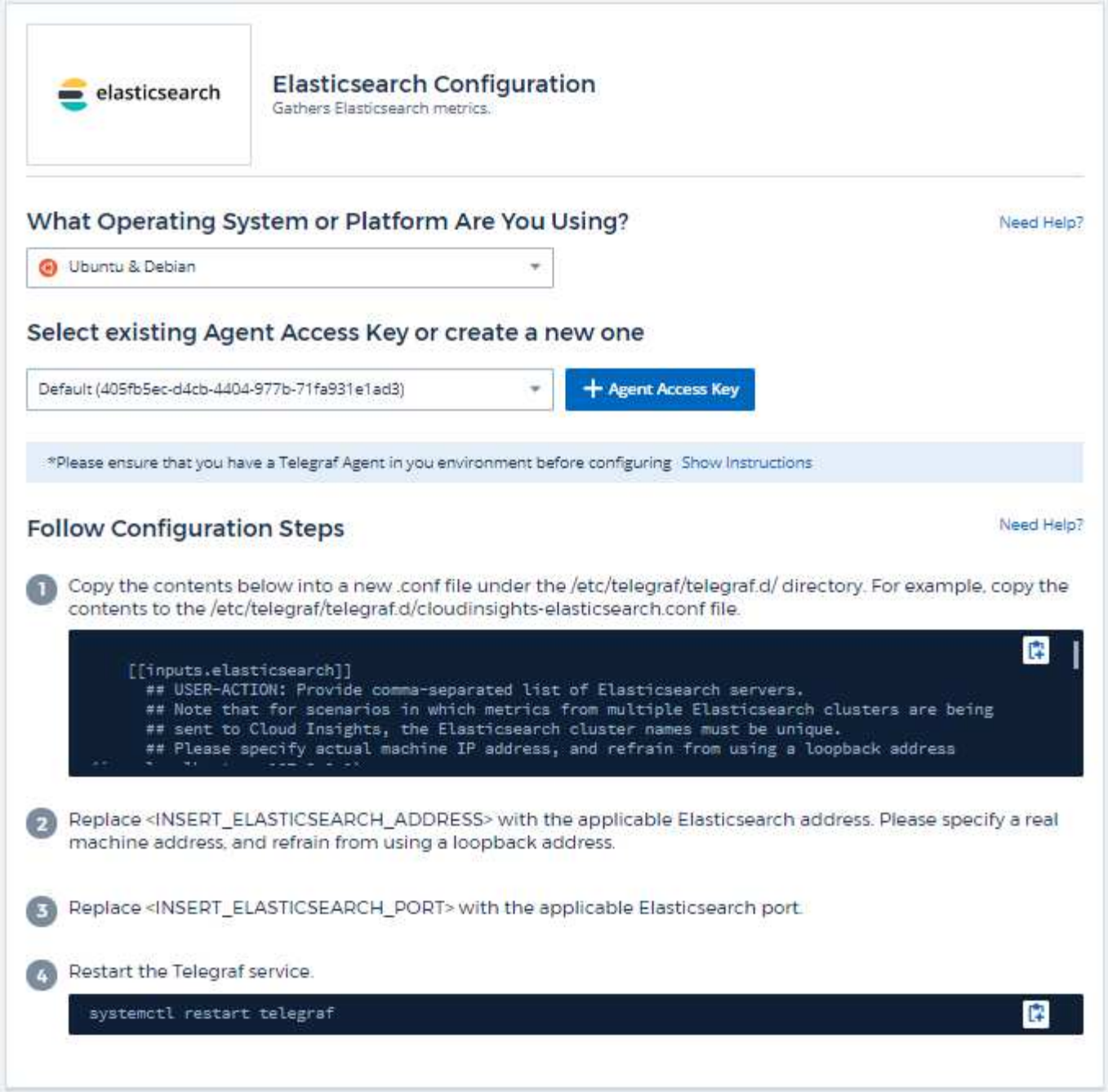
Raccoglitore dati Elasticsearch

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Elasticsearch.

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Elasticsearch.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione di Elasticsearch" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:
Cluster Elasticsearch	Cluster di spazi dei nomi	IP del nodo Nome del nodo Stato del cluster
Nodo Elasticsearch	Cluster dello spazio dei nomi ID nodo ES IP nodo ES Nodo ES	ID zona

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Flink Data Collector

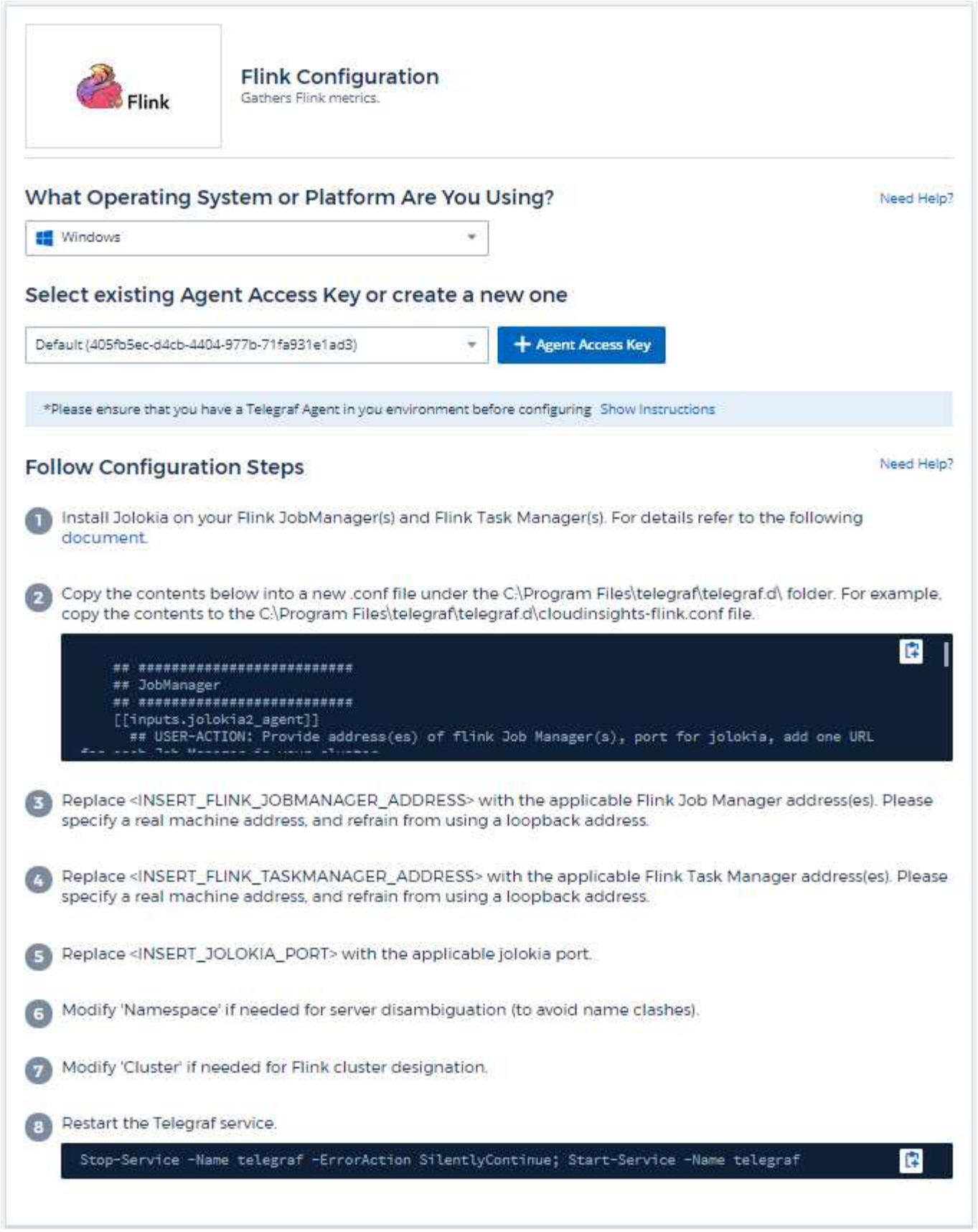
Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Flink.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Flink.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Una distribuzione completa di Flink prevede i seguenti componenti:

JobManager: il sistema primario Flink. Coordina una serie di TaskManager. In una configurazione ad alta disponibilità, il sistema avrà più di un JobManager. TaskManager: è qui che vengono eseguiti gli operatori Flink. Il plugin Flink è basato sul plugin Jolokia di Telegraf. Poiché è un requisito per raccogliere informazioni da tutti i componenti Flink, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata per la versione 1.7.0 di Flink.

Impostazione

Barattolo dell'agente Jolokia

Per tutti i singoli componenti è necessario scaricare una versione del file jar dell'agente Jolokia. La versione testata era"Agente Jolokia 1.6.0" .

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jolokia-jvm-1.6.0-agent.jar) sia posizionato nel percorso '/opt/flink/lib/'.

Gestore di lavori

Per configurare JobManager in modo che esponga l'API Jolokia, puoi impostare la seguente variabile di ambiente sui tuoi nodi, quindi riavviare JobManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Puoi scegliere una porta diversa per Jolokia (8778).  Se hai un IP interno
su cui bloccare Jolokia, puoi sostituire "catch all" 0.0.0.0 con il tuo
IP.  Si noti che questo IP deve essere accessibile dal plugin Telegraf.
```

Task Manager

Per configurare TaskManager in modo che esponga l'API Jolokia, puoi impostare la seguente variabile di ambiente sui tuoi nodi, quindi riavviare TaskManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Puoi scegliere una porta diversa per Jolokia (8778).  Se hai un IP interno
su cui bloccare Jolokia, puoi sostituire "catch all" 0.0.0.0 con il tuo
IP.  Si noti che questo IP deve essere accessibile dal plugin Telegraf.
```

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Gestore attività Flink	Server dello spazio dei nomi del cluster	Nome nodo ID Task Manager IP nodo	Segmenti di memoria disponibili in rete Segmenti di memoria totali in rete Garbage Collection PS MarkSweep Count Tempo di Garbage Collection PS MarkSweep Count Scavenge PS Garbage Collection PS Scavenge Count Tempo di Scavenge PS Garbage Collection Heap Memory Memoria Heap impegnata Heap di inizializzazione Heap Memory massima utilizzata Thread Count Thread Daemon Count Thread di picco Thread Count Totale avviato
Lavoro Flink	ID processo del server dello spazio dei nomi del cluster	Nome nodo Nome lavoro IP nodo Ultimo checkpoint Percorso esterno Ora di riavvio	Tempo di inattività Riavvii completi Allineamento ultimo checkpoint Durata ultimo checkpoint in buffer Dimensione ultimo checkpoint Numero di checkpoint completati Numero di checkpoint non riusciti Numero di checkpoint in corso Numero di checkpoint Tempo di attività

Oggetto:	Identificatori:	Attributi:	Punti dati:
Gestore di lavori Flink	Server dello spazio dei nomi del cluster	Nome nodo IP nodo	Conteggio PS MarkSweep di Garbage Collection Tempo PS MarkSweep di Garbage Collection Conteggio PS Scavenge di Garbage Collection Tempo PS Scavenge di Garbage Collection Memoria heap Memoria heap impegnata Memoria heap di inizializzazione Memoria heap massima utilizzata Numero di task manager registrati Numero di processi in esecuzione Slot attività Slot attività disponibili Conteggio thread totale Conteggio thread daemon Conteggio thread di picco Conteggio thread totale avviato

Oggetto:	Identificatori:	Attributi:	Punti dati:
Compito Flink	ID lavoro spazio dei nomi cluster ID attività	Nome nodo server Nome lavoro Indice sottoattività ID tentativo attività Numero tentativo attività Nome attività ID gestore attività IP nodo Input corrente Filigrana	Utilizzo del pool di buffer Lunghezza della coda di buffer Utilizzo del pool di buffer Lunghezza della coda di buffer Numero buffer in locale Numero buffer in locale al secondo Conteggio Numero buffer in locale al secondo Numero buffer in remoto Numero buffer in remoto al secondo Conteggio Numero buffer in remoto al secondo Numero buffer in uscita Numero buffer in uscita al secondo Conteggio Numero buffer in uscita al secondo Numero byte in locale Numero byte in locale al secondo Conteggio Numero byte in locale al secondo Numero byte in remoto Numero byte in remoto al secondo Conteggio Numero byte in remoto al secondo Numero byte in uscita Numero byte in uscita al secondo Conteggio Numero byte in uscita al secondo Numero record in ingresso Numero record in ingresso al secondo Numero record in ingresso al secondo Numero record in uscita Numero record in uscita al secondo Numero record in uscita al secondo

Oggetto:	Identificatori:	Attributi:	Punti dati:
Operatore di attività Flink	ID lavoro spazio dei nomi cluster ID operatore ID attività	Nome nodo server Nome lavoro Nome operatore Indice sottoattività ID tentativo attività Numero tentativo attività Nome attività ID gestore attività IP nodo	Filigrana di input corrente Filigrana di output corrente Numero record in ingresso Numero record in ingresso al secondo Conteggio Numero record in ingresso al secondo Numero record in uscita Numero record in uscita al secondo Conteggio Numero record in uscita al secondo Numero record in ritardo eliminati Partizioni assegnate Byte consumati Tasso Latenza commit Latenza commit media Tasso massimo commit Commit non riusciti Commit riusciti Tasso di chiusura connessione Conteggio connessioni Tasso di creazione connessione Conteggio Latenza fetch media Latenza fetch massima Tasso fetch Dimensione fetch Dimensione fetch media Tempo massimo di limitazione fetch Tempo medio di limitazione fetch Frequenza heartbeat massima Frequenza byte in ingresso Rapporto IO Tempo IO medio (ns) Rapporto di attesa IO Tempo di attesa IO medio (ns) Frequenza di unione Tempo di unione Ultimo heartbeat medio fa Frequenza IO di rete Tasso byte in uscita Record consumati Tasso Ritardo record Record massimi per richiesta Tasso medio di richiesta Dimensione richiesta Dimensione media richiesta Frequenza di risposta massima Seleziona frequenza Frequenza di sincronizzazione Tempo di sincronizzazione Tempo medio di risposta heartbeat Tempo di

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati Hadoop

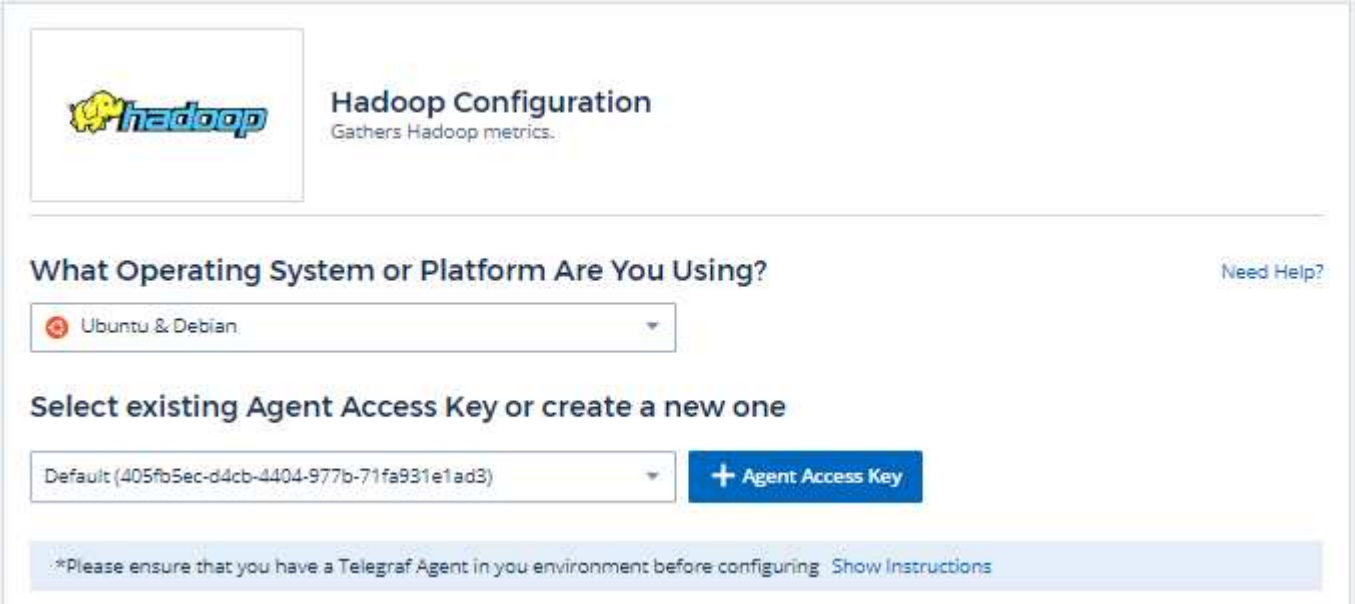
Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Hadoop.

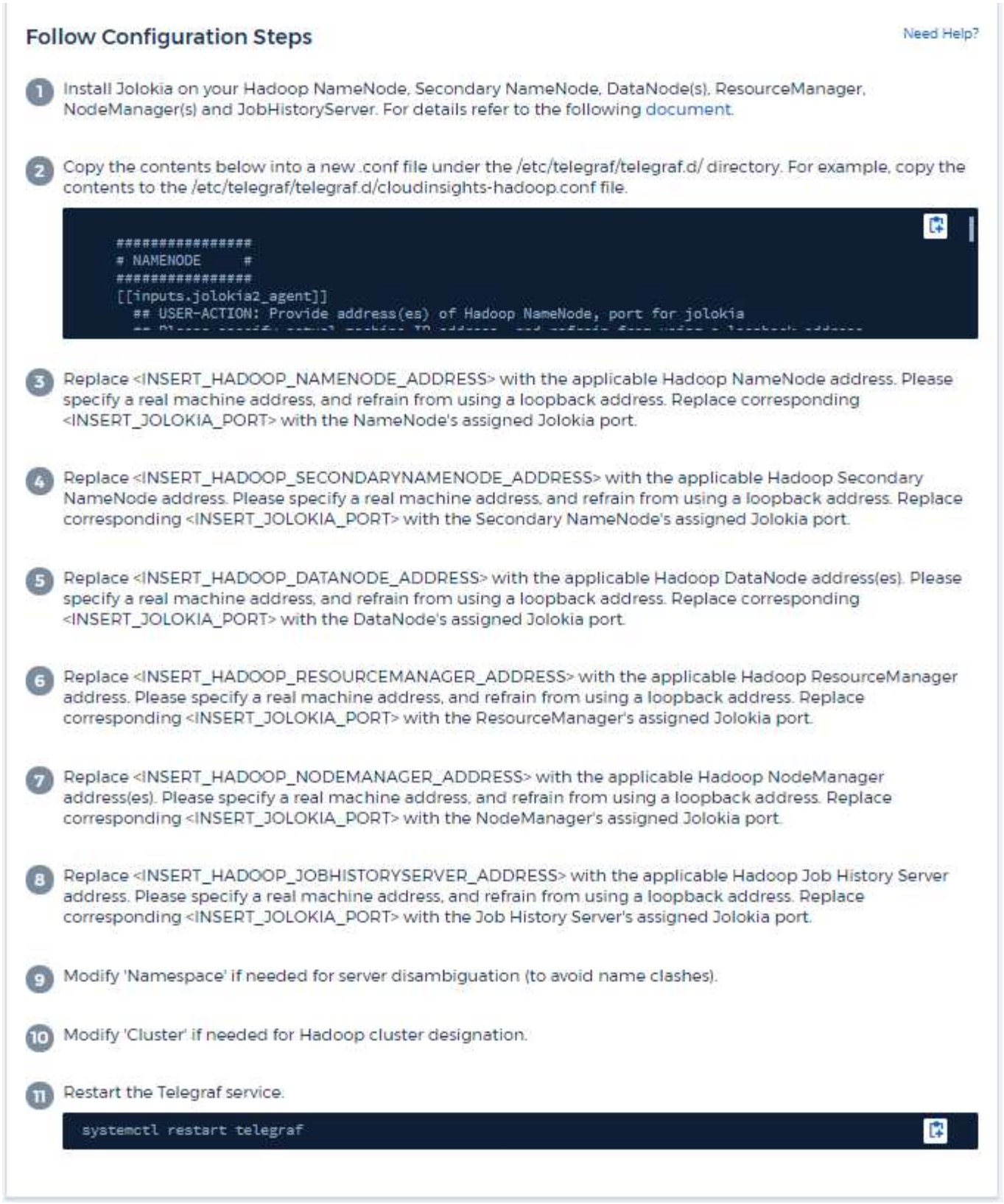
Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Hadoop.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.





Impostare

Una distribuzione completa di Hadoop prevede i seguenti componenti:

- NameNode: il sistema primario del file system distribuito Hadoop (HDFS). Coordina una serie di DataNode.

- NameNode secondario: un failover a caldo per il NameNode principale. In Hadoop la promozione a NameNode non avviene automaticamente. Il NameNode secondario raccoglie informazioni dal NameNode per essere pronto a essere promosso quando necessario.
- DataNode: Proprietario effettivo dei dati.
- ResourceManager: il sistema di elaborazione primario (Yarn). Coordina una serie di NodeManager.
- NodeManager: la risorsa per il calcolo. Posizione effettiva per l'esecuzione delle applicazioni.
- JobHistoryServer: responsabile della gestione di tutte le richieste relative alla cronologia dei lavori.

Il plugin Hadoop è basato sul plugin Jolokia di Telegraf. Poiché è un requisito per raccogliere informazioni da tutti i componenti Hadoop, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata per Hadoop versione 2.9.2.

Impostazione

Barattolo dell'agente Jolokia

Per tutti i singoli componenti è necessario scaricare una versione del file jar dell'agente Jolokia. La versione testata era"Agente Jolokia 1.6.0" .

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jolokia-jvm-1.6.0-agent.jar) sia posizionato nel percorso '/opt/hadoop/lib/'.

NomeNodo

Per configurare NameNode in modo che esponga l'API Jolokia, puoi impostare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nome secondarioNodo

Per configurare il Secondary NameNode in modo che esponga l'API Jolokia, puoi impostare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nodo dati

Per configurare i DataNode in modo che espongano l'API Jolokia, puoi impostare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

ResourceManager

Per configurare ResourceManager in modo che esponga l'API Jolokia, puoi impostare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Gestore dei nodi

Per configurare i NodeManager in modo che espongano l'API Jolokia, puoi impostare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

JobHistoryServer

Per configurare JobHistoryServer in modo che esponga l'API Jolokia, è possibile impostare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:
Nome secondario HadoopNode	Server dello spazio dei nomi del cluster	Nome nodo IP nodo Informazioni di compilazione Versione
Hadoop NodeManager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo
Hadoop Resource Manager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo
Hadoop DataNode	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID cluster Versione
Nome nodo Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID transazione Ultima scrittura Ora dall'ultimo caricamento Modifiche Stato HA Stato del file system ID del pool di blocchi ID del cluster Informazioni sulla compilazione Conteggio distinta delle versioni Versione
Hadoop JobHistoryServer	Server dello spazio dei nomi del cluster	Nome nodo IP nodo

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati HAProxy

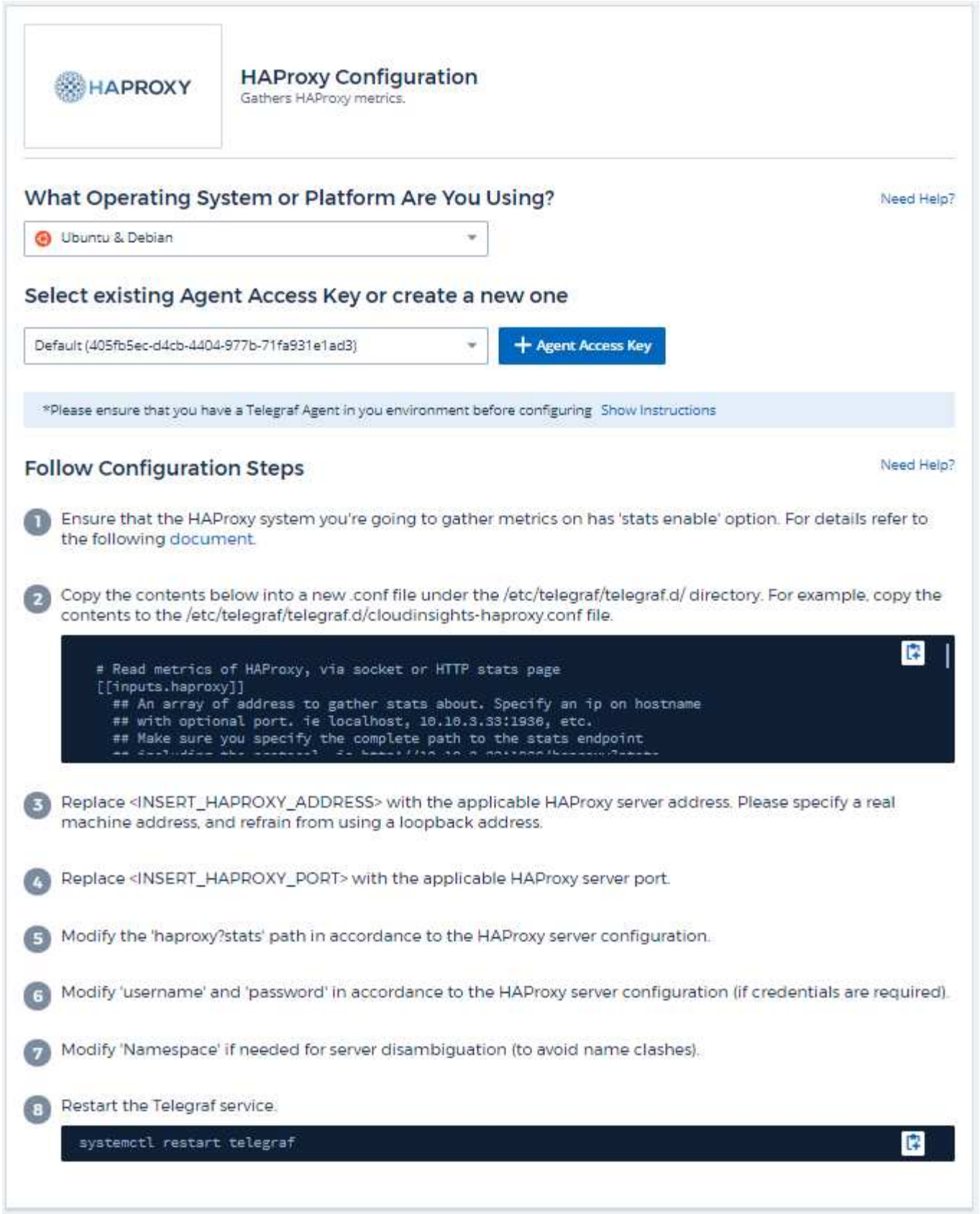
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da HAProxy.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli HAProxy.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Il plugin di Telegraf per HAProxy si basa sull'abilitazione di HAProxy Stats. Questa è una configurazione integrata in HAProxy, ma non è abilitata di default. Se abilitato, HAProxy esporrà un endpoint HTML che può

essere visualizzato sul browser o recuperato per l'estrazione dello stato di tutte le configurazioni HAProxy.

Compatibilità:

La configurazione è stata sviluppata per HAProxy versione 1.9.4.

Impostazione:

Per abilitare le statistiche, modifica il file di configurazione haproxy e aggiungi le seguenti righe dopo la sezione 'defaults', utilizzando il tuo nome utente/password e/o l'URL haproxy:

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

Di seguito è riportato un esempio semplificato di file di configurazione con statistiche abilitate:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Per istruzioni complete e aggiornate, consultare il"Documentazione HAProxy" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Frontend HAProxy	Proxy indirizzo spazio dei nomi	IP nodo Nome nodo ID proxy Modalità ID processo Sessioni Limite velocità ID server Limite sessioni Stato	Byte in entrata Byte in uscita Cache Hits Cache Lookups Compressione Byte bypassati Compressione Byte in entrata Compressione Byte in uscita Compressione Risposte Velocità di connessione Velocità di connessione Connessioni massime Totale richieste rifiutate dalla regola di connessione Richieste rifiutate per problemi di sicurezza Risposte rifiutate per problemi di sicurezza Richieste rifiutate dalla regola di sessione Richieste Errori Risposte Risposte 1xx Risposte 2xx Risposte 3xx Risposte 4xx Risposte 5xx Altre richieste Sessioni intercettate Velocità sessioni Velocità richieste massime Velocità richieste Velocità richieste massime Totale sessioni Sessioni Sessioni massime Totale richieste Riscritture

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server HAProxy	Server proxy indirizzo spazio dei nomi	IP del nodo Nome del nodo Controlla ora di fine Controlla configurazione caduta Controlla valore integrità Controlla configurazione salita Controlla stato ID proxy Ora ultima modifica Ora ultima sessione Modalità ID processo ID server Stato Peso	Server attivi Server di backup Byte in entrata Byte in uscita Controlli inattivi Controlli non riusciti Client interrompe Connessioni Tempo medio di connessione Tempo di inattività Totale risposte negate Errori di connessione Errori di risposta Risposte 1xx Risposte 2xx Risposte 3xx Risposte 4xx Risposte 5xx Altro server selezionato Coda totale Coda corrente Tempo medio massimo della coda Sessioni al secondo Sessioni al secondo Tempo massimo di riutilizzo della connessione Tempo di risposta Media sessioni Sessioni Massimo trasferimento server Interruzioni sessioni Totale sessioni Tempo medio totale Richieste Ridistribuzioni Richieste Nuovi tentativi Richieste Riscritture

Oggetto:	Identificatori:	Attributi:	Punti dati:
Backend HAProxy	Proxy indirizzo spazio dei nomi	IP nodo Nome nodo ID proxy Ora ultima modifica Ora ultima sessione Modalità ID processo ID server Limite sessioni Stato Peso	Server attivi Server di backup Byte in entrata Byte in uscita Cache Hit Cache Lookup Check Down Client Abort Compressione Byte bypassati Compressione Byte in entrata Compressione Byte in uscita Compressione Risposte Connessioni Tempo medio di connessione Tempo di inattività Richieste totali negate per problemi di sicurezza Risposte negate per problemi di sicurezza Errori di connessione Errori di risposta Risposte 1xx Risposte 2xx Risposte 3xx Risposte 4xx Risposte 5xx Altro server selezionato Coda totale Coda corrente Coda massima Tempo medio Sessioni al secondo Sessioni al secondo Richieste massime Riutilizzo della connessione Tempo di risposta Media sessioni Sessioni Massima server Trasferimento Abort Sessioni Sessioni totali Tempo totale Richieste medie Ridistribuzioni Richieste Nuovi tentativi Richieste Riscritture

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati JVM

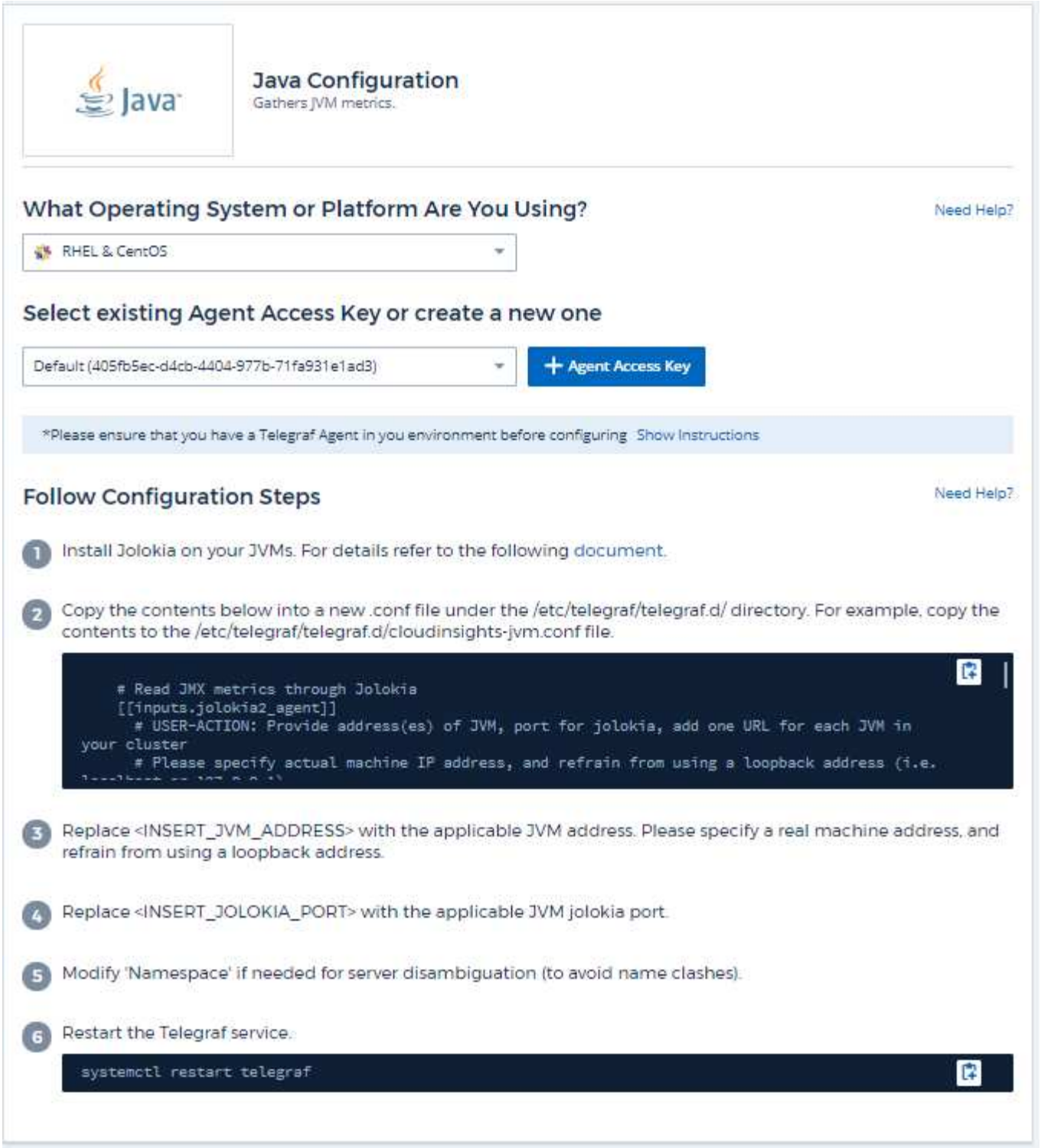
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da JVM.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli JVM.

Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate in"Documentazione JVM" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
JVM	JVM dello spazio dei nomi	Architettura del sistema operativo Nome del sistema operativo Versione del sistema operativo Specifiche di runtime Fornitore delle specifiche di runtime Versione delle specifiche di runtime Tempo di attività Nome della VM di runtime Fornitore della VM di runtime Versione della VM di runtime Nome del nodo IP del nodo	Classe caricata Classe caricata Totale Classe scaricata Heap di memoria impegnato Heap di memoria inizializzato Heap di memoria utilizzato Heap di memoria massimo utilizzato Memoria non heap impegnata Memoria non heap inizializzato Memoria non heap massima Memoria non heap utilizzata Oggetti di memoria in attesa di finalizzazione Processori del sistema operativo disponibili Dimensione della memoria virtuale impegnata del sistema operativo Dimensione della memoria fisica libera del sistema operativo Dimensione dello spazio di swap libero del sistema operativo Conteggio massimo dei descrittori di file del sistema operativo Conteggio dei descrittori di file aperti del sistema operativo Carico CPU del processore del sistema operativo Tempo CPU del processore del sistema operativo Carico CPU del sistema del sistema operativo Carico medio del sistema operativo Dimensione totale della memoria fisica del sistema operativo Dimensione totale dello spazio di swap del sistema operativo Conteggio dei daemon dei thread Conteggio dei picchi dei thread Conteggio dei thread Conteggio totale dei thread avviati Conteggio della raccolta copie del Garbage Collector Tempo di raccolta copie del Garbage Collector Conteggio della raccolta Mark-sweep del Garbage

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore di dati Kafka

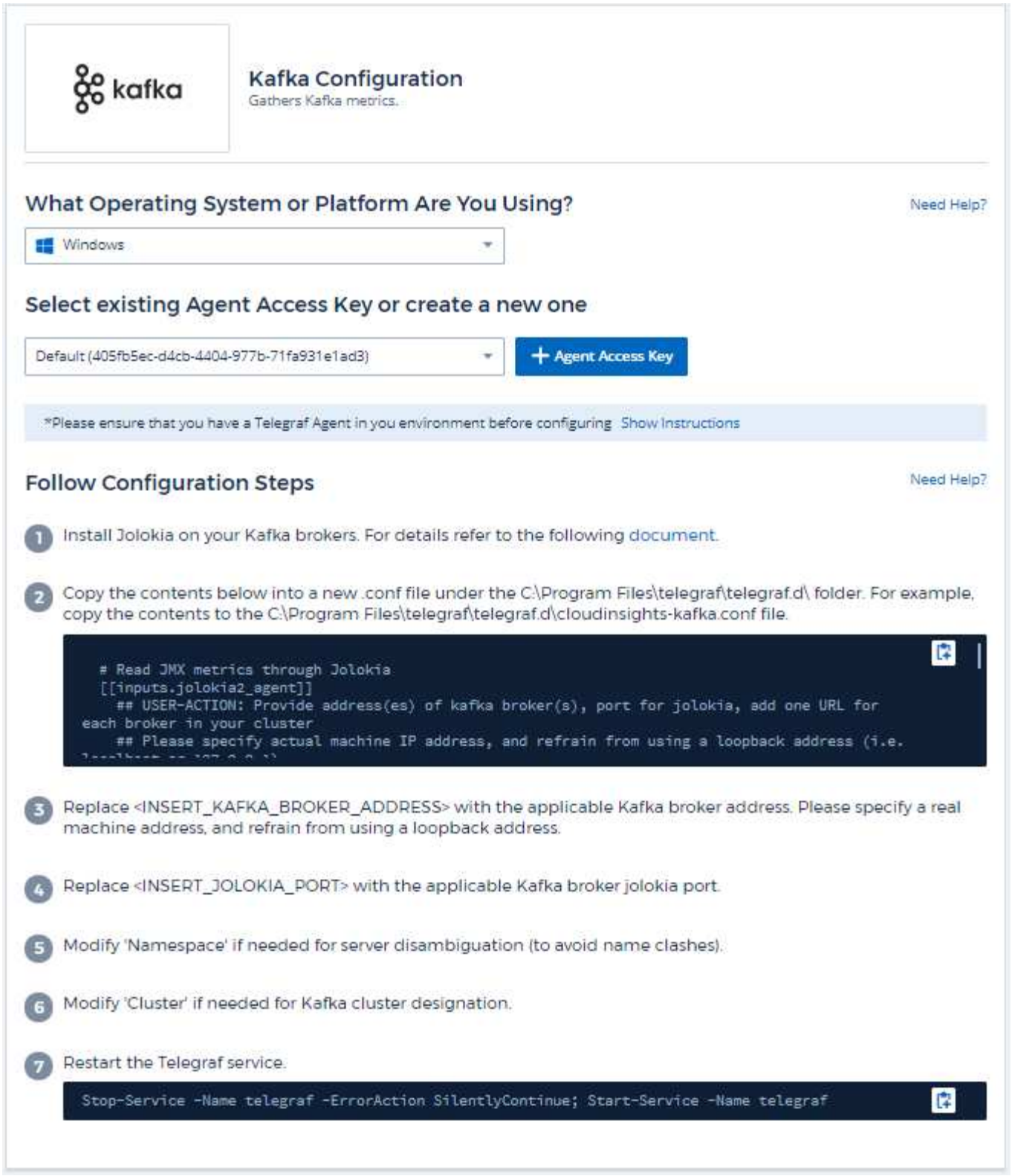
Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Kafka.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Kafka.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Il plugin Kafka è basato sul plugin Jolokia di Telegraf. Poiché è un requisito per raccogliere informazioni da tutti i broker Kafka, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata per la versione 0.11.0.2 di Kafka.

Impostazione

Tutte le istruzioni riportate di seguito presuppongono che il percorso di installazione di Kafka sia '/opt/kafka'. Puoi adattare le istruzioni riportate di seguito in base alla tua posizione di installazione.

Barattolo dell'agente Jolokia

Una versione del file jar dell'agente Jolokia deve essere"scaricato" . La versione testata era Jolokia Agent 1.6.0.

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jolokia-jvm-1.6.0-agent.jar) si trovi nel percorso '/opt/kafka/libs/'.

Kafka Brokers

Per configurare Kafka Brokers in modo che esponga l'API Jolokia, puoi aggiungere quanto segue in <KAFKA_HOME>/bin/kafka-server-start.sh, subito prima della chiamata 'kafka-run-class.sh':

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Si noti che nell'esempio precedente si utilizza 'hostname -I' per impostare la variabile di ambiente 'RMI_HOSTNAME'. Nelle macchine con più IP, sarà necessario apportare modifiche per raccogliere l'IP di interesse per le connessioni RMI.

È possibile scegliere una porta diversa per JMX (9999 sopra) e Jolokia (8778). Se hai un IP interno su cui bloccare Jolokia, puoi sostituire "catch all" 0.0.0.0 con il tuo IP. Si noti che questo IP deve essere accessibile dal plugin Telegraf. Se non si desidera eseguire l'autenticazione, è possibile utilizzare l'opzione '-Dcom.sun.management.jmxremote.authenticate=false'. Da utilizzare a proprio rischio e pericolo.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:
Kafka Broker	Cluster Namespace Broker	Nome nodo IP nodo

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Kibana Data Collector

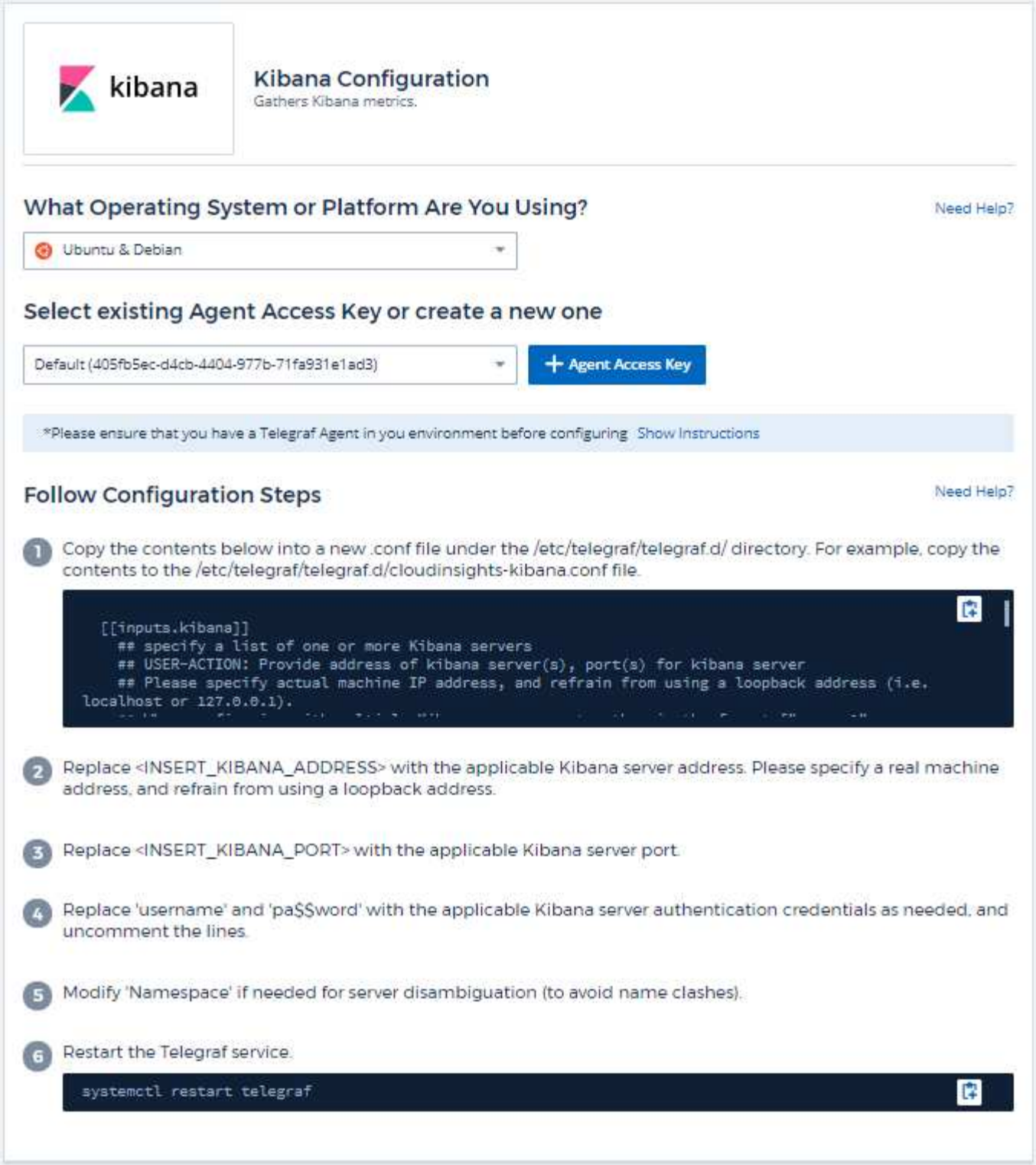
Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Kibana.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Kibana.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione Kibana" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Kibana	Indirizzo dello spazio dei nomi	IP del nodo Nome del nodo Versione Stato	Heap di connessioni simultanee Heap massimo utilizzato Richieste al secondo Tempo di risposta Tempo di risposta medio Tempo di attività massimo

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

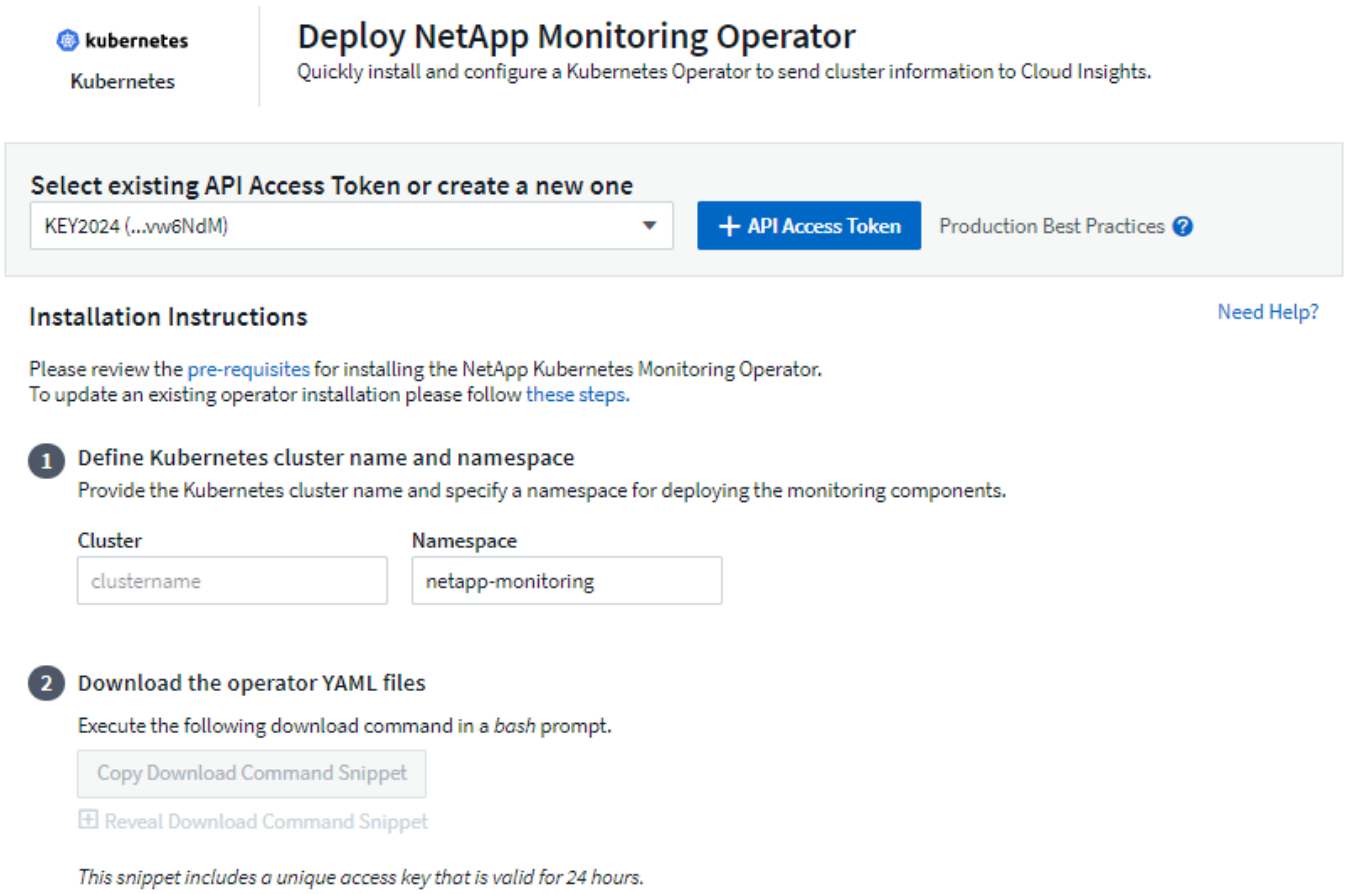
Installazione e configurazione dell'operatore di monitoraggio Kubernetes

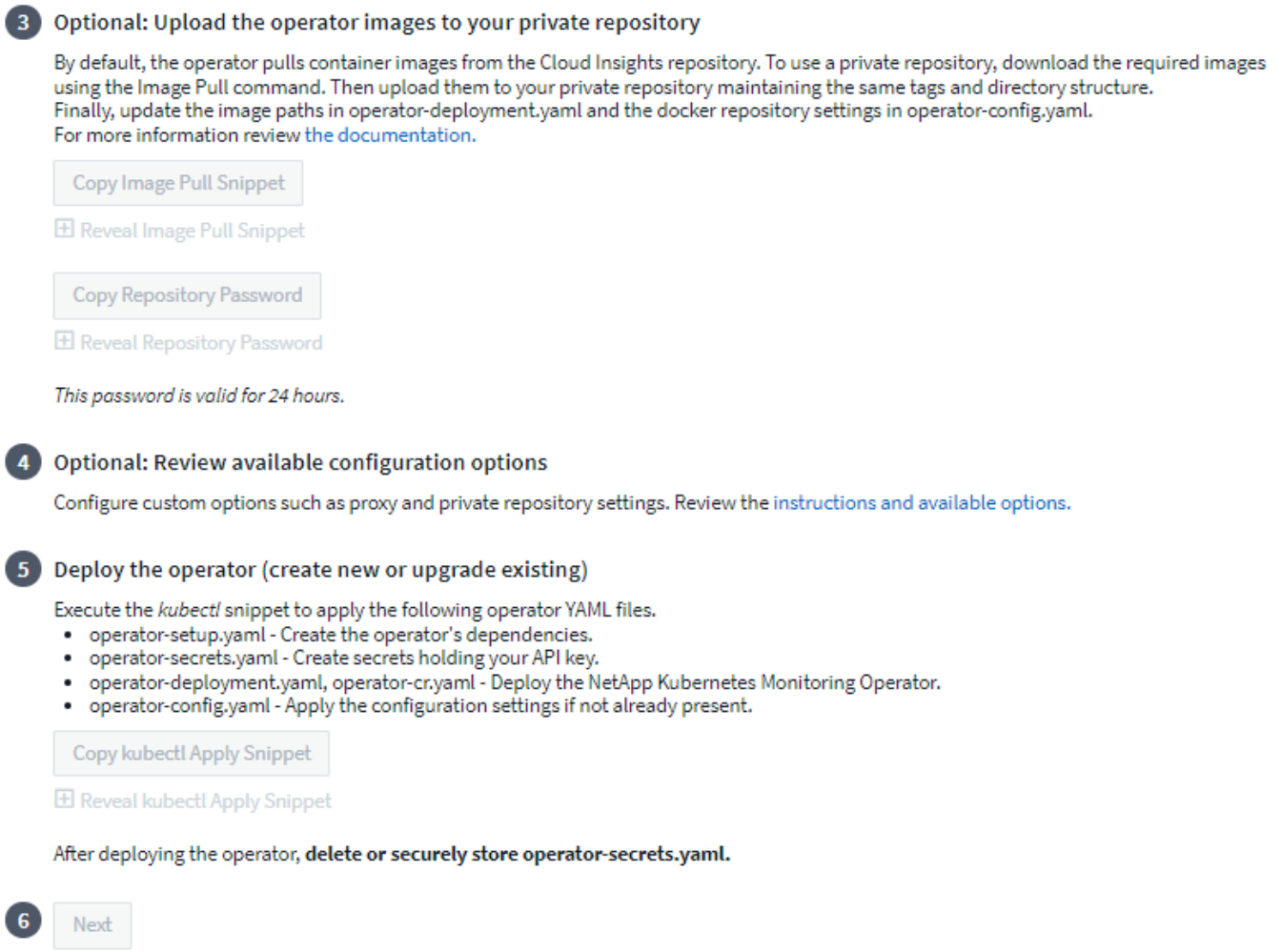
Data Infrastructure Insights offre l'**operatore di monitoraggio Kubernetes** per la raccolta Kubernetes. Passare a **Kubernetes > Collectors > +Kubernetes Collector** per distribuire un nuovo operatore.

Prima di installare Kubernetes Monitoring Operator

Vedi il"Prerequisiti" documentazione prima di installare o aggiornare Kubernetes Monitoring Operator.

Installazione dell'operatore di monitoraggio Kubernetes





Passaggi per installare l'agente Kubernetes Monitoring Operator su Kubernetes:

1. Immettere un nome cluster e uno spazio dei nomi univoci. Se seiaggiornamento da un precedente operatore Kubernetes, utilizzare lo stesso nome del cluster e lo stesso spazio dei nomi.
2. Una volta inseriti questi dati, è possibile copiare il frammento del comando Download negli appunti.
3. Incolla lo snippet in una finestra *bash* ed eseguilo. Verranno scaricati i file di installazione dell'operatore. Si noti che lo snippet ha una chiave univoca ed è valido per 24 ore.
4. Se hai un repository personalizzato o privato, copia il frammento di codice Image Pull facoltativo, incollalo in una shell *bash* ed eseguilo. Una volta estratte le immagini, copiale nel tuo repository privato. Assicuratevi di mantenere gli stessi tag e la stessa struttura delle cartelle. Aggiornare i percorsi in *operator-deployment.yaml* e le impostazioni del repository Docker in *operator-config.yaml*.
5. Se lo si desidera, rivedere le opzioni di configurazione disponibili, come le impostazioni del proxy o del repository privato. Puoi leggere di più su"opzioni di configurazione" .
6. Quando sei pronto, distribuisci l'operatore copiando lo snippet Apply di kubectl, scaricandolo ed eseguendolo.
7. L'installazione procede automaticamente. Una volta completato, fare clic sul pulsante *Avanti*.
8. Al termine dell'installazione, fare clic sul pulsante *Avanti*. Assicurati di eliminare o archiviare in modo sicuro anche il file *operator-secrets.yaml*.

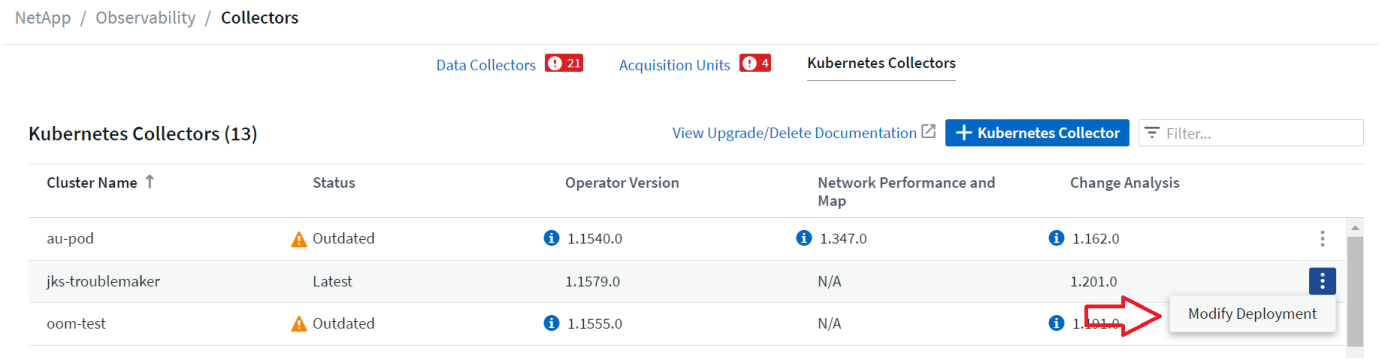
Se hai un repository personalizzato, leggi a riguardoutilizzando un repository Docker personalizzato/privato .

Componenti di monitoraggio di Kubernetes

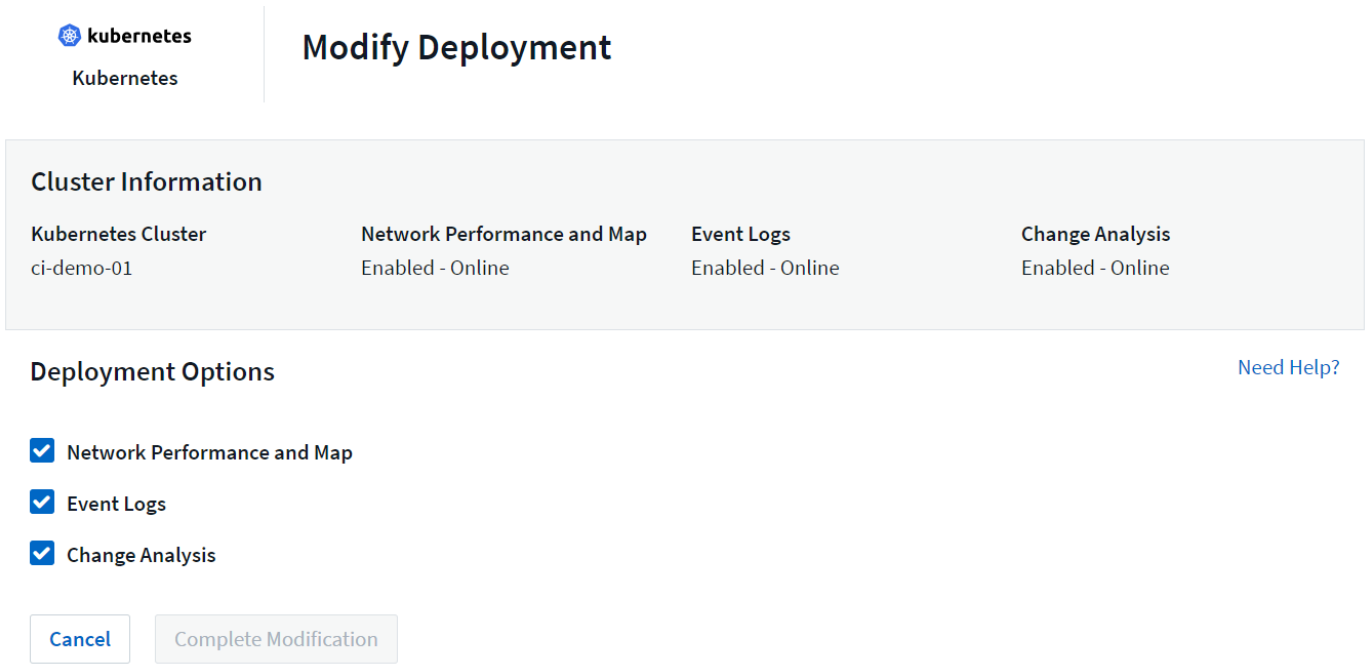
Data Infrastructure Insights Kubernetes Monitoring è composto da quattro componenti di monitoraggio:

- Metriche del cluster
- Prestazioni di rete e mappa (facoltativo)
- Registri eventi (facoltativo)
- Analisi del cambiamento (facoltativo)

I componenti facoltativi sopra indicati sono abilitati per impostazione predefinita per ciascun collector Kubernetes; se decidi che non hai bisogno di un componente per un collector specifico, puoi disabilitarlo andando su **Kubernetes > Collectors** e selezionando *Modifica distribuzione* dal menu "tre punti" del collector sulla destra dello schermo.



La schermata mostra lo stato attuale di ciascun componente e consente di disabilitare o abilitare i componenti per quel raccoglitore, a seconda delle necessità.



Aggiornamento all'ultima versione di Kubernetes Monitoring Operator

Aggiornamenti dei pulsanti DII

È possibile aggiornare Kubernetes Monitoring Operator tramite la pagina DII Kubernetes Collectors. Fare clic sul menu accanto al cluster che si desidera aggiornare e selezionare *Aggiorna*. L'operatore verificherà le firme delle immagini, eseguirà uno snapshot dell'installazione corrente ed eseguirà l'aggiornamento. Entro pochi minuti dovresti vedere l'avanzamento dello Stato dell'operatore da Aggiornamento in corso a Ultimo. Se si verifica un errore, è possibile selezionare lo stato Errore per maggiori dettagli e fare riferimento alla tabella di risoluzione dei problemi degli aggiornamenti tramite pulsante riportata di seguito.

Aggiornamenti rapidi con repository privati

Se il tuo operatore è configurato per utilizzare un repository privato, assicurati che tutte le immagini necessarie per eseguire l'operatore e le relative firme siano disponibili nel tuo repository. Se durante il processo di aggiornamento si verifica un errore per immagini mancanti, è sufficiente aggiungerle al repository e riprovare l'aggiornamento. Per caricare le firme delle immagini nel tuo repository, utilizza lo strumento di co-firma come segue, assicurandoti di caricare le firme per tutte le immagini specificate in 3 Facoltativo: carica le immagini dell'operatore nel tuo repository privato > Frammento di estrazione dell'immagine

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Ripristino di una versione precedentemente in esecuzione

Se hai effettuato l'aggiornamento utilizzando la funzionalità di aggiornamento tramite pulsante e riscontri difficoltà con la versione corrente dell'operatore entro sette giorni dall'aggiornamento, puoi effettuare il downgrade alla versione in esecuzione in precedenza utilizzando lo snapshot creato durante il processo di aggiornamento. Fare clic sul menu accanto al cluster di cui si desidera eseguire il rollback e selezionare *Roll back*.

Aggiornamenti manuali

Determinare se esiste un *AgentConfiguration* con l'operatore esistente (se il namespace non è il *netapp-monitoring* predefinito, sostituire il namespace appropriato):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Se esiste un _AgentConfiguration_:
```

- Installarel'ultimo Operatore rispetto all'Operatore esistente.
  - Assicurati di essereestrazione delle ultime immagini del contenitore se si utilizza un repository personalizzato.

Se *AgentConfiguration* non esiste:

- Prendi nota del nome del tuo cluster riconosciuto da Data Infrastructure Insights (se il tuo namespace non è quello predefinito netapp-monitoring, sostituiscilo con il namespace appropriato):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Crea un backup dell'operatore esistente (se il tuo namespace non è il
netapp-monitoring predefinito, sostituiscilo con il namespace
appropriato):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-
operator,Disinstallare>>l'operatore esistente.
* <<installing-the-kubernetes-monitoring-operator,Installare>>l'ultimo
Operatore.
```

- Utilizzare lo stesso nome del cluster.
- Dopo aver scaricato gli ultimi file YAML dell'Operator, trasferisci tutte le personalizzazioni trovate in *agent_backup.yaml* nel *operator-config.yaml* scaricato prima della distribuzione.
- Assicurati di essereestrazione delle ultime immagini del contenitore se si utilizza un repository personalizzato.

Arresto e avvio dell'operatore di monitoraggio Kubernetes

Per arrestare Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Per avviare Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Disinstallazione

Per rimuovere l'operatore di monitoraggio Kubernetes

Si noti che lo spazio dei nomi predefinito per l'operatore di monitoraggio Kubernetes è "netapp-monitoring". Se hai impostato un tuo namespace, sostituiscilo in questi e in tutti i comandi e file successivi.

Le versioni più recenti dell'operatore di monitoraggio possono essere disinstallate con i seguenti comandi:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Se l'operatore di monitoraggio è stato distribuito nel proprio namespace dedicato, eliminare il namespace:

```
 kubectl delete ns <NAMESPACE>
Nota: se il primo comando restituisce "Nessuna risorsa trovata",
utilizzare le seguenti istruzioni per disinstallare le versioni precedenti
dell'operatore di monitoraggio.
```

Eseguire ciascuno dei seguenti comandi nell'ordine indicato. A seconda dell'installazione corrente, alcuni di questi comandi potrebbero restituire messaggi di tipo "oggetto non trovato". Questi messaggi possono essere tranquillamente ignorati.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Se in precedenza è stato creato un vincolo di contesto di sicurezza:

```
kubectl delete scc telegraf-hostaccess
```

Informazioni su Kube-state-metrics

NetApp Kubernetes Monitoring Operator installa le proprie metriche kube-state per evitare conflitti con altre istanze.

Per informazioni su Kube-State-Metrics, vedere"questa pagina" .

Configurazione/Personalizzazione dell'operatore

Queste sezioni contengono informazioni sulla personalizzazione della configurazione dell'operatore, sull'utilizzo del proxy, sull'utilizzo di un repository Docker personalizzato o privato o sull'utilizzo di OpenShift.

Opzioni di configurazione

Le impostazioni modificate più comunemente possono essere configurate nella risorsa personalizzata *AgentConfiguration*. È possibile modificare questa risorsa prima di distribuire l'operatore modificando il file *operator-config.yaml*. Questo file include esempi di impostazioni commentati. Vedi l'elenco di"impostazioni disponibili" per la versione più recente dell'operatore.

È anche possibile modificare questa risorsa dopo aver distribuito l'operatore utilizzando il seguente comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Per determinare se la versione distribuita dell'operatore supporta
_AgentConfiguration_, eseguire il seguente comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se viene visualizzato il messaggio "Errore dal server (NotFound)", è
necessario aggiornare l'operatore prima di poter utilizzare
AgentConfiguration.
```

Configurazione del supporto proxy

Esistono due posti in cui è possibile utilizzare un proxy sul tenant per installare Kubernetes Monitoring Operator. Possono essere gli stessi sistemi proxy o sistemi proxy separati:

- Proxy necessario durante l'esecuzione dello snippet di codice di installazione (utilizzando "curl") per connettere il sistema in cui viene eseguito lo snippet al tuo ambiente Data Infrastructure Insights
- Proxy necessario al cluster Kubernetes di destinazione per comunicare con l'ambiente Data Infrastructure Insights

Se si utilizza un proxy per uno o entrambi questi elementi, per installare Kubernetes Operating Monitor è necessario innanzitutto assicurarsi che il proxy sia configurato per consentire una buona comunicazione con l'ambiente Data Infrastructure Insights . Se disponi di un proxy e puoi accedere a Data Infrastructure Insights dal server/VM da cui desideri installare l'operatore, è probabile che il tuo proxy sia configurato correttamente.

Per il proxy utilizzato per installare Kubernetes Operating Monitor, prima di installare l'operatore, impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare anche la variabile di ambiente *no_proxy*.

Per impostare le variabili, esegui i seguenti passaggi sul tuo sistema **prima** di installare Kubernetes Monitoring Operator:

1. Imposta le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:
   a. Se il proxy da configurare non dispone di autenticazione (nome utente/password), eseguire il seguente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Se il proxy da configurare dispone di autenticazione (nome
utente/password), eseguire questo comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Per far sì che il proxy utilizzato per il cluster Kubernetes comunichi con l'ambiente Data Infrastructure Insights , installare Kubernetes Monitoring Operator dopo aver letto tutte queste istruzioni.

Configura la sezione proxy di *AgentConfiguration* in *operator-config.yaml* prima di distribuire Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utilizzo di un repository Docker personalizzato o privato

Per impostazione predefinita, Kubernetes Monitoring Operator estrarrà le immagini dei container dal repository Data Infrastructure Insights . Se si utilizza un cluster Kubernetes come destinazione per il monitoraggio e tale cluster è configurato per estrarre immagini di container solo da un repository Docker personalizzato o privato o da un registro di container, è necessario configurare l'accesso ai container necessari all'operatore di monitoraggio Kubernetes.

Eseguire "Image Pull Snippet" dal riquadro di installazione di NetApp Monitoring Operator. Questo comando effettuerà l'accesso al repository Data Infrastructure Insights , estrarrà tutte le dipendenze delle immagini per l'operatore e uscirà dal repository Data Infrastructure Insights . Quando richiesto, immettere la password temporanea del repository fornita. Questo comando scarica tutte le immagini utilizzate dall'operatore, comprese quelle per le funzionalità opzionali. Di seguito sono riportate le funzioni per cui vengono utilizzate queste immagini.

Funzionalità dell'operatore principale e monitoraggio di Kubernetes

- monitoraggio netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf

- utente root senza distribuzione

Registro eventi

- ci-fluent-bit
- ci-kubernetes-event-exporter

Prestazioni e mappa della rete

- ci-net-observer

Invia l'immagine Docker dell'operatore al tuo repository Docker privato/locale/aziendale in base alle policy aziendali. Assicurati che i tag delle immagini e i percorsi delle directory di queste immagini nel tuo repository siano coerenti con quelli nel repository Data Infrastructure Insights .

Modifica la distribuzione monitoring-operator in operator-deployment.yaml e modifica tutti i riferimenti alle immagini per utilizzare il tuo repository Docker privato.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modifica *AgentConfiguration* in *operator-config.yaml* per riflettere la nuova posizione del docker repo. Crea un nuovo imagePullSecret per il tuo repository privato, per maggiori dettagli vedi *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Token di accesso API per password a lungo termine

Alcuni ambienti (ad esempio repository proxy) richiedono password a lungo termine per il Data Infrastructure Insights docker repository. La password fornita nell'interfaccia utente al momento dell'installazione è valida solo per 24 ore. Invece di utilizzare quella, si può usare un API Access Token come password del docker repository. Questa password sarà valida finché l'API Access Token sarà valido. Si può generare un nuovo API Access Token per questo scopo specifico o utilizzarne uno esistente.

"Leggi qui" per istruzioni su come creare un nuovo token di accesso API.

Per estrarre un API Access Token esistente da un file *operator-secrets.yaml* scaricato, gli utenti possono eseguire quanto segue:

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

Per estrarre un API Access Token esistente da un'installazione dell'operatore in esecuzione, gli utenti possono eseguire quanto segue:

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

Istruzioni OpenShift

Se si utilizza OpenShift 4.6 o versioni successive, è necessario modificare *AgentConfiguration* in *operator-config.yaml* per abilitare l'impostazione *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift potrebbe implementare un livello di sicurezza aggiuntivo che potrebbe bloccare l'accesso ad alcuni componenti di Kubernetes.

Tolleranze e difetti

I DaemonSet *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* e *netapp-ci-net-observer-l4-ds* devono pianificare un pod su ogni nodo del cluster per raccogliere correttamente i dati su tutti i nodi. L'operatore è stato configurato per tollerare alcune **imperfezioni** ben note. Se hai configurato delle taint personalizzate sui tuoi nodi, impedendo così ai pod di essere eseguiti su ogni nodo, puoi creare una **tolleranza** per quelle taint"nella *AgentConfiguration*" . Se hai applicato taint personalizzati a tutti i nodi del tuo cluster, devi anche aggiungere le tolleranze necessarie alla distribuzione dell'operatore per consentire la pianificazione e l'esecuzione del pod dell'operatore.

Scopri di più su Kubernetes"Contaminazioni e tolleranze" .

Ritorno al"* Pagina di installazione dell'operatore di monitoraggio NetApp Kubernetes*"

Una nota sui segreti

Per rimuovere l'autorizzazione per l'operatore di monitoraggio Kubernetes a visualizzare i segreti a livello di cluster, eliminare le seguenti risorse dal file *operator-setup.yaml* prima dell'installazione:

```
ClusterRole/netapp-ci<namespace>-agent-secret
ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

Se si tratta di un aggiornamento, elimina anche le risorse dal tuo cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Se l'analisi delle modifiche è abilitata, modificare *AgentConfiguration* o *operator-config.yaml* per rimuovere il commento dalla sezione change-management e includere *kindsToIgnoreFromWatch: '"secrets"'* nella sezione change-management. Notare la presenza e la posizione delle virgolette singole e doppie in questa riga.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Verifica delle firme delle immagini degli operatori di monitoraggio di Kubernetes

L'immagine per l'operatore e tutte le immagini correlate che distribuisce sono firmate da NetApp. È possibile verificare manualmente le immagini prima dell'installazione utilizzando lo strumento di co-firma oppure configurare un controller di ammissione Kubernetes. Per maggiori dettagli si prega di consultare il"Documentazione di Kubernetes" .

La chiave pubblica utilizzata per verificare le firme delle immagini è disponibile nel riquadro di installazione dell'operatore di monitoraggio in *Facoltativo: carica le immagini dell'operatore nel tuo repository privato > Chiave pubblica della firma dell'immagine*

Per verificare manualmente una firma immagine, procedere come segue:

1. Copia ed esegui l'Image Pull Snippet
2. Copia e inserisci la password del repository quando richiesto
3. Memorizza la chiave pubblica della firma dell'immagine (dii-image-signing.pub nell'esempio)
4. Verificare le immagini tramite co-firma. Fare riferimento al seguente esempio di utilizzo del cosign

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi durante la configurazione dell'operatore di monitoraggio Kubernetes:

Problema:	Prova questo:
Non vedo alcun collegamento ipertestuale/connessione tra il mio volume persistente Kubernetes e il dispositivo di archiviazione back-end corrispondente. Il mio volume persistente Kubernetes è configurato utilizzando il nome host del server di archiviazione.	Seguire i passaggi per disinstallare l'agente Telegraf esistente, quindi reinstallare l'agente Telegraf più recente. È necessario utilizzare Telegraf versione 2.0 o successiva e l'archiviazione del cluster Kubernetes deve essere monitorata attivamente da Data Infrastructure Insights.

Problema:	Prova questo:
Nei log vedo messaggi simili ai seguenti: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.MutatingWebhookConfiguration: il server non è riuscito a trovare la risorsa richiesta E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.Lease: il server non è riuscito a trovare la risorsa richiesta (ottenere leases.coordination.k8s.io) ecc.	Questi messaggi possono essere visualizzati se si esegue kube-state-metrics versione 2.0.0 o successiva con versioni di Kubernetes precedenti alla 1.20. Per ottenere la versione di Kubernetes: *kubectl version* Per ottenere la versione di kube-state-metrics: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Per evitare che questi messaggi si verifichino, gli utenti possono modificare la distribuzione di kube-state-metrics per disabilitare i seguenti lease: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Più specificamente, possono utilizzare il seguente argomento CLI: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, secrets,services,statefulsets,storageclasses L’elenco di risorse predefinito è: "certificatesigningrequests,configmaps,cronjobs,daemonsets,deployments, endpoints,horizontalpodautoscalers,ingresses,jobs,leases,limitranges, mutatingwebhookconfigurations,namespaces,networkpolicies,nodes, persistentvolumeclaims,persistentvolumes,poddisruptionbudgets,pods,replicasets, replicationcontrollers,resourcequotas,secrets,services, statefulsets,storageclasses, validatingwebhookconfigurations,volumeattachments"

Problema:	Prova questo:
Vedo messaggi di errore da Telegraf simili ai seguenti, ma Telegraf si avvia ed è in esecuzione: 11 ott 14:23:41 ip-172-31-39-47 systemd[1]: Avviato L'agente server basato su plugin per la segnalazione delle metriche in InfluxDB. 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="impossibile creare la directory della cache. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: permesso negato. ignorato\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="apertura non riuscita. Ignorato. Apri /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: nessun file o directory\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z I! Avvio di Telegraf 1.19.3	Questo è un problema noto. Fare riferimento a"Questo articolo di GitHub" per maggiori dettagli. Finché Telegraf è attivo e funzionante, gli utenti possono ignorare questi messaggi di errore.
Su Kubernetes, i miei pod Telegraf segnalano il seguente errore: "Errore nell'elaborazione delle informazioni mountstats: impossibile aprire il file mountstats: /hostfs/proc/1/mountstats, errore: apertura /hostfs/proc/1/mountstats: autorizzazione negata"	Se SELinux è abilitato e applicato, è probabile che impedisca ai pod Telegraf di accedere al file /proc/1/mountstats sul nodo Kubernetes. Per superare questa restrizione, modificare agentconfiguration e abilitare l'impostazione runPrivileged. Per maggiori dettagli, fare riferimento alle istruzioni di OpenShift.
Su Kubernetes, il mio pod Telegraf ReplicaSet segnala il seguente errore: [inputs.prometheus] Errore nel plugin: impossibile caricare la coppia di chiavi /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: aprire /etc/kubernetes/pki/etcd/server.crt: nessun file o directory del genere	Il pod Telegraf ReplicaSet è progettato per essere eseguito su un nodo designato come master o per etcd. Se il pod ReplicaSet non è in esecuzione su uno di questi nodi, verranno visualizzati questi errori. Controlla se i tuoi nodi master/etcd presentano delle anomalie. In tal caso, aggiungere le tolleranze necessarie al Telegraf ReplicaSet, telegraf-rs. Ad esempio, modifica ReplicaSet… kubectl edit rs telegraf-rs …e aggiungi le tolleranze appropriate alla specifica. Quindi, riavviare il pod ReplicaSet.

Problema:	Prova questo:
Ho un ambiente PSP/PSA. Ciò ha ripercussioni sul mio operatore di monitoraggio?	Se il cluster Kubernetes è in esecuzione con Pod Security Policy (PSP) o Pod Security Admission (PSA), è necessario eseguire l'aggiornamento alla versione più recente di Kubernetes Monitoring Operator. Per effettuare l'aggiornamento all'operatore corrente con supporto per PSP/PSA, seguire questi passaggi: 1. Disinstallare l'operatore di monitoraggio precedente: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installare l'ultima versione dell'operatore di monitoraggio.
Ho riscontrato problemi nel tentativo di distribuire l'Operatore e sto utilizzando PSP/PSA.	1. Modificare l'agente utilizzando il seguente comando: kubectl -n <name-space> edit agent 2. Contrassegna 'security-policy-enabled' come 'false'. In questo modo verranno disattivati i criteri di sicurezza del Pod e l'ammissione di sicurezza del Pod e sarà consentito all'operatore di effettuare la distribuzione. Confermare utilizzando i seguenti comandi: kubectl get psp (dovrebbe mostrare che la politica di sicurezza del pod è stata rimossa) kubectl get all -n <namespace>
grep -i psp (dovrebbe mostrare che non è stato trovato nulla)	Errori "ImagePullBackoff" rilevati
Questi errori potrebbero verificarsi se si dispone di un repository Docker personalizzato o privato e non è ancora stato configurato Kubernetes Monitoring Operator per riconoscerlo correttamente. Per saperne di più sulla configurazione per repository personalizzati/privati.	Ho un problema con la distribuzione del mio operatore di monitoraggio e la documentazione attuale non mi aiuta a risolverlo.

Problema:	Prova questo:

Acquisire o annotare in altro modo l'output dei seguenti comandi e contattare il team di supporto tecnico.
 	
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	I pod net-observer (Workload Map) nello spazio dei nomi Operator sono in CrashLoopBackOff

Questi pod corrispondono al raccoglitore di dati Workload Map per Network Observability. Prova questi: • Controlla i log di uno dei pod per confermare la versione minima del kernel. Ad esempio: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"fallimento nella convalida. Motivo: la versione del kernel 3.10.0 è inferiore alla versione minima del kernel 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • I pod Net-observer richiedono che la versione del kernel Linux sia almeno 4.18.0. Controllare la versione del kernel utilizzando il comando "uname -r" e assicurarsi che sia >= 4.18.0	I pod sono in esecuzione nello spazio dei nomi Operatore (predefinito: netapp-monitoring), ma nell'interfaccia utente non vengono visualizzati dati per la mappa del carico di lavoro o metriche Kubernetes nelle query
Controllare l'impostazione dell'ora sui nodi del cluster K8S. Per un audit e una segnalazione dei dati accurati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'agente utilizzando il protocollo NTP (Network Time Protocol) o il protocollo SNTP (Simple Network Time Protocol).	Alcuni dei pod net-observer nello spazio dei nomi Operator sono nello stato In sospeso
Net-observer è un DaemonSet ed esegue un pod in ogni nodo del cluster k8s. • Prendi nota del pod che si trova nello stato In sospeso e controlla se sta riscontrando un problema di risorse per la CPU o la memoria. Assicurarsi che nel nodo siano disponibili la memoria e la CPU richieste.	Subito dopo aver installato Kubernetes Monitoring Operator, vedo quanto segue nei miei log: [inputs.prometheus] Errore nel plugin: errore durante la richiesta HTTP a http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Ottieni http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: dial tcp: cerca kube-state-metrics.<namespace>.svc.cluster.local: nessun host del genere

Problema:	Prova questo:
In genere questo messaggio viene visualizzato solo quando viene installato un nuovo operatore e il pod *telegraf-rs* è attivo prima del pod *ksm*. Questi messaggi dovrebbero cessare una volta che tutti i pod saranno in esecuzione.	Non vedo alcuna metrica raccolta per i CronJob di Kubernetes presenti nel mio cluster.
Verifica la tua versione di Kubernetes (ad esempio `kubectl version`). Se la versione è v1.20.x o precedente, si tratta di una limitazione prevista. La versione kube-state-metrics distribuita con Kubernetes Monitoring Operator supporta solo v1.CronJob. Con Kubernetes 1.20.x e versioni precedenti, la risorsa CronJob si trova in v1beta.CronJob. Di conseguenza, kube-state-metrics non riesce a trovare la risorsa CronJob.	Dopo aver installato l'operatore, i pod telegraf-ds entrano in CrashLoopBackOff e i log dei pod indicano "su: Authentication failure".
Modifica la sezione telegraf in *AgentConfiguration* e imposta *dockerMetricCollectionEnabled* su false. Per maggiori dettagli, fai riferimento a "opzioni di configurazione" dell'operatore. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Nei miei registri di Telegraf vedo messaggi di errore ricorrenti simili ai seguenti: E! [agente] Errore durante la scrittura su output.http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": scadenza del contesto superata (Client.Timeout superato durante l'attesa delle intestazioni)
Modificare la sezione telegraf in *AgentConfiguration* e aumentare *outputTimeout* a 10 s. Per maggiori dettagli fare riferimento al manuale dell'operatore"opzioni di configurazione" .	Mancano i dati *involvedobject* per alcuni registri eventi.
Assicurati di aver seguito i passaggi indicati in"Permessi" sezione sopra.	Perché vedo due pod di operatori di monitoraggio in esecuzione, uno denominato netapp-ci-monitoring-operator-<pod> e l'altro denominato monitoring-operator-<pod>?
A partire dal 12 ottobre 2023, Data Infrastructure Insights ha riorganizzato l'operatore per servire meglio i nostri utenti; affinché tali modifiche vengano adottate completamente, è necessariorimuovere il vecchio operatore Einstallare quello nuovo .	I miei eventi Kubernetes hanno smesso inaspettatamente di segnalare a Data Infrastructure Insights.
Recupera il nome del pod event-exporter: `` `kubectl -n netapp-monitoring get pods ``	grep event-exporter

Problema:	Prova questo:
awk '{print $1}'	sed 's/event-exporter./event-exporter/` Dovrebbe essere "netapp-ci-event-exporter" o "event-exporter". Successivamente, modifica l'agente di monitoraggio `kubectl -n netapp-monitoring edit agent` e impostare il valore per LOG_FILE in modo che rifletta il nome appropriato del pod di esportazione eventi trovato nel passaggio precedente. Più specificatamente, LOG_FILE dovrebbe essere impostato su "/var/log/containers/netapp-ci-event-exporter.log" o "/var/log/containers/event-exporter*.log" …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. In alternativa, si può anchedisinstallare Ereinstallare l'agente.
Vedo che i pod distribuiti dal Kubernetes Monitoring Operator si bloccano a causa di risorse insufficienti.	Fare riferimento all'operatore di monitoraggio Kubernetes"opzioni di configurazione" per aumentare i limiti della CPU e/o della memoria secondo necessità.
Un'immagine mancante o una configurazione non valida hanno impedito l'avvio o la disponibilità dei pod netapp-ci-kube-state-metrics. Ora StatefulSet è bloccato e le modifiche alla configurazione non vengono applicate ai pod netapp-ci-kube-state-metrics.	Lo StatefulSet è in un"rotto" stato. Dopo aver risolto eventuali problemi di configurazione, riavviare i pod netapp-ci-kube-state-metrics.
I pod netapp-ci-kube-state-metrics non riescono ad avviarsi dopo aver eseguito un aggiornamento dell'operatore Kubernetes, generando l'errore ErrImagePull (impossibilità di estrarre l'immagine).	Prova a reimpostare manualmente i pod.
Durante l'analisi dei log, vengono visualizzati i messaggi "Evento scartato perché più vecchio di maxEventAgeSeconds" per il mio cluster Kubernetes.	Modificare l'operatore *agentconfiguration* e aumentare *event-exporter-maxEventAgeSeconds* (ad esempio a 60 s), *event-exporter-kubeQPS* (ad esempio a 100) e *event-exporter-kubeBurst* (ad esempio a 500). Per maggiori dettagli su queste opzioni di configurazione, vedere"opzioni di configurazione" pagina.

Problema:	Prova questo:
Telegraf avvisa o si blocca a causa di una memoria bloccabile insufficiente.	Prova ad aumentare il limite di memoria bloccabile per Telegraf nel sistema operativo/nodo sottostante. Se aumentare il limite non è un'opzione, modificare la configurazione dell'agente NKMO e impostare *unprotected* su *true*. Ciò indicherà a Telegraf di non tentare di riservare pagine di memoria bloccate. Sebbene ciò possa rappresentare un rischio per la sicurezza, in quanto i segreti decrittati potrebbero essere trasferiti su disco, consente l'esecuzione in ambienti in cui non è possibile riservare memoria bloccata. Per maggiori dettagli sulle opzioni di configurazione *non protette*, fare riferimento a"opzioni di configurazione" pagina.
Vedo messaggi di avviso da Telegraf simili ai seguenti: *W! [inputs.diskio] Impossibile raccogliere il nome del disco per "vdc": errore durante la lettura di /dev/vdc: nessun file o directory del genere*	Per il Kubernetes Monitoring Operator, questi messaggi di avviso sono benigni e possono essere ignorati senza problemi. In alternativa, modifica la sezione telegraf in AgentConfiguration e imposta *runDsPrivileged* su true. Per maggiori dettagli, consulta il "opzioni di configurazione dell'operatore".

Problema:	Prova questo:

Il mio pod fluent-bit non funziona con i seguenti errori: [2024/10/16 14:16:23] [errore] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Troppi file aperti [2024/10/16 14:16:23] [errore] inizializzazione input tail.0 non riuscita [2024/10/16 14:16:23] [errore] [motore] inizializzazione input non riuscita	Prova a modificare le impostazioni *fsnotify* nel tuo cluster:
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	Riavvia Fluent-bit.
	Nota: per rendere queste impostazioni persistenti tra i riavvii del nodo, è necessario inserire le seguenti righe in */etc/sysctl.conf*
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problema:	Prova questo:
I pod DS di Telegraf segnalano errori relativi al plugin di input Kubernetes che non riesce a effettuare richieste HTTP a causa dell’impossibilità di convalidare il certificato TLS. Ad esempio: E! [inputs.kubernetes] Errore nel plugin: errore durante la richiesta HTTP a"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Ottenere"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: impossibile verificare il certificato: x509: impossibile convalidare il certificato per <kubelet_IP> perché non contiene alcun IP SAN	Ciò si verifica se il kubelet utilizza certificati autofirmati e/o il certificato specificato non include <kubelet_IP> nell'elenco *Subject Alternative Name* dei certificati. Per risolvere questo problema, l'utente può modificare il"configurazione dell'agente" e impostare *telegraf:insecureK8sSkipVerify* su *true*. In questo modo il plugin di input Telegraf verrà configurato per saltare la verifica. In alternativa, l'utente può configurare il kubelet per"serverTLSBootstrap" , che attiverà una richiesta di certificato dall'API 'certificates.k8s.io'.
Ricevo il seguente errore nei pod Fluent-bit e il pod non può essere avviato: 026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	Assicurarsi che la directory host in cui risiede il file DB disponga dei permessi di lettura/scrittura appropriati. Più specificamente, la directory host dovrebbe concedere permessi di lettura/scrittura agli utenti non root. Il percorso predefinito del file DB è /var/log/ a meno che non venga sovrascritto dall'opzione fluent-bit-dbFile *agentconfiguration*. Se SELinux è abilitato, provare a impostare l'opzione fluent-bit-seLinuxOptionsType agentconfiguration su 'spc_t'

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Memcached Data Collector

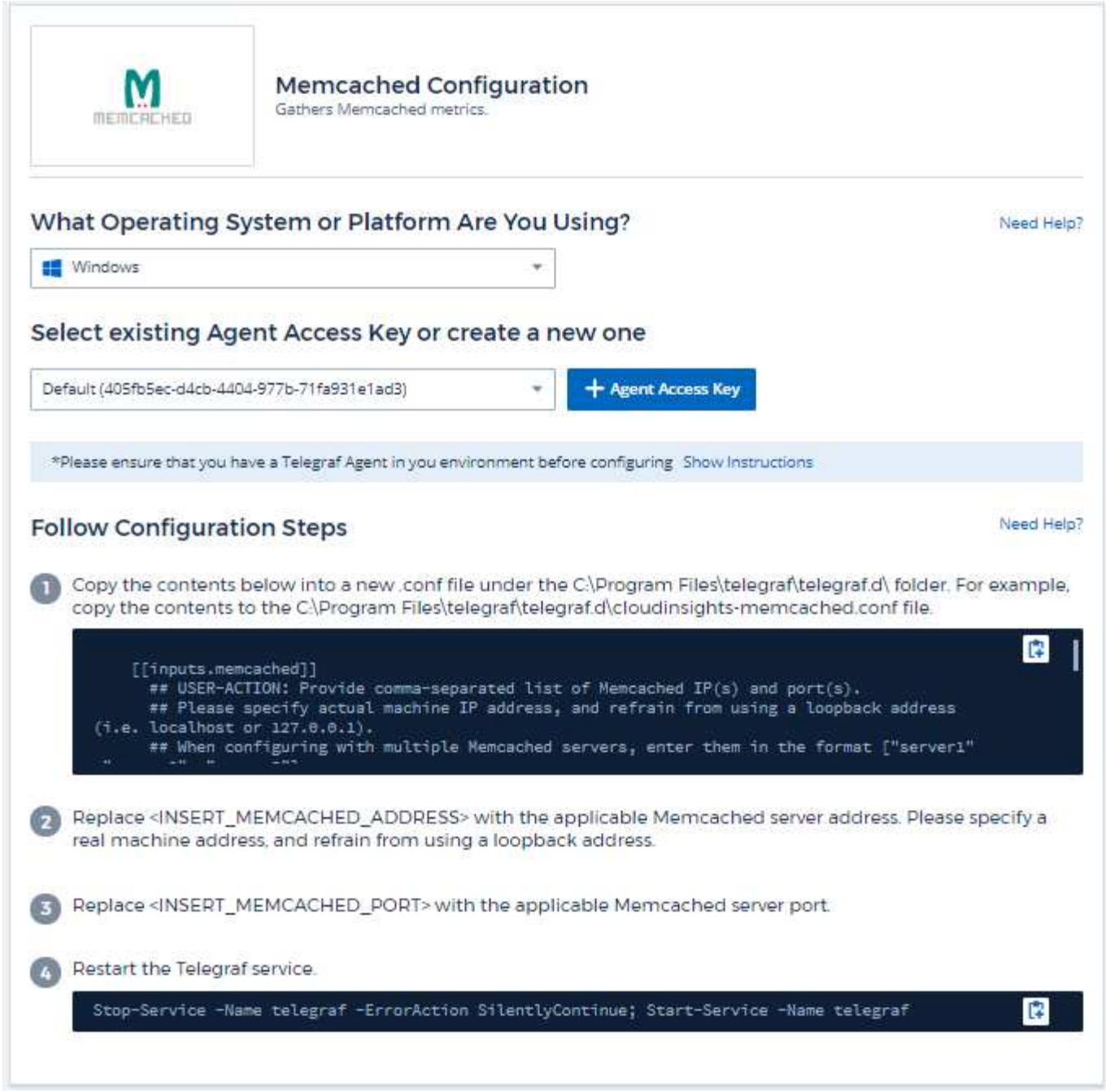
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Memcached.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Memcached.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Wiki di Memcached" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Memcached	Server dello spazio dei nomi	IP del nodo Nome del nodo	Accettazione di connessioni Gestite Richieste di autenticazione Autenticazioni non riuscite Byte utilizzati Byte letti (al sec) Byte scritti (al sec) CAS Badval CAS Hit CAS Misses Richieste di svuotamento (al sec) Richieste di ottenimento (al sec) Richieste di impostazione (al sec) Richieste di tocco (al sec) Rendimenti di connessione (al sec) Strutture di connessione Connessioni aperte Elementi archiviati correnti Richieste di decr Hit (al sec) Richieste di decr Misses (al sec) Richieste di eliminazione Hit (al sec) Richieste di eliminazione Misses (al sec) Elementi espulsi Espulsioni valide Elementi scaduti Hit di ottenimento (al sec) Misses di ottenimento (al sec) Byte hash utilizzati L'hash è in espansione Livello di potenza hash Richieste di incremento Hit (al sec) Richieste di incremento Misses (al sec) Byte massimi del server Ascolto disabilitato Numero thread worker recuperati Conteggio Totale connessioni aperte Totale elementi archiviati Hit di tocco Misses di tocco Tempo di attività del server

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati MongoDB

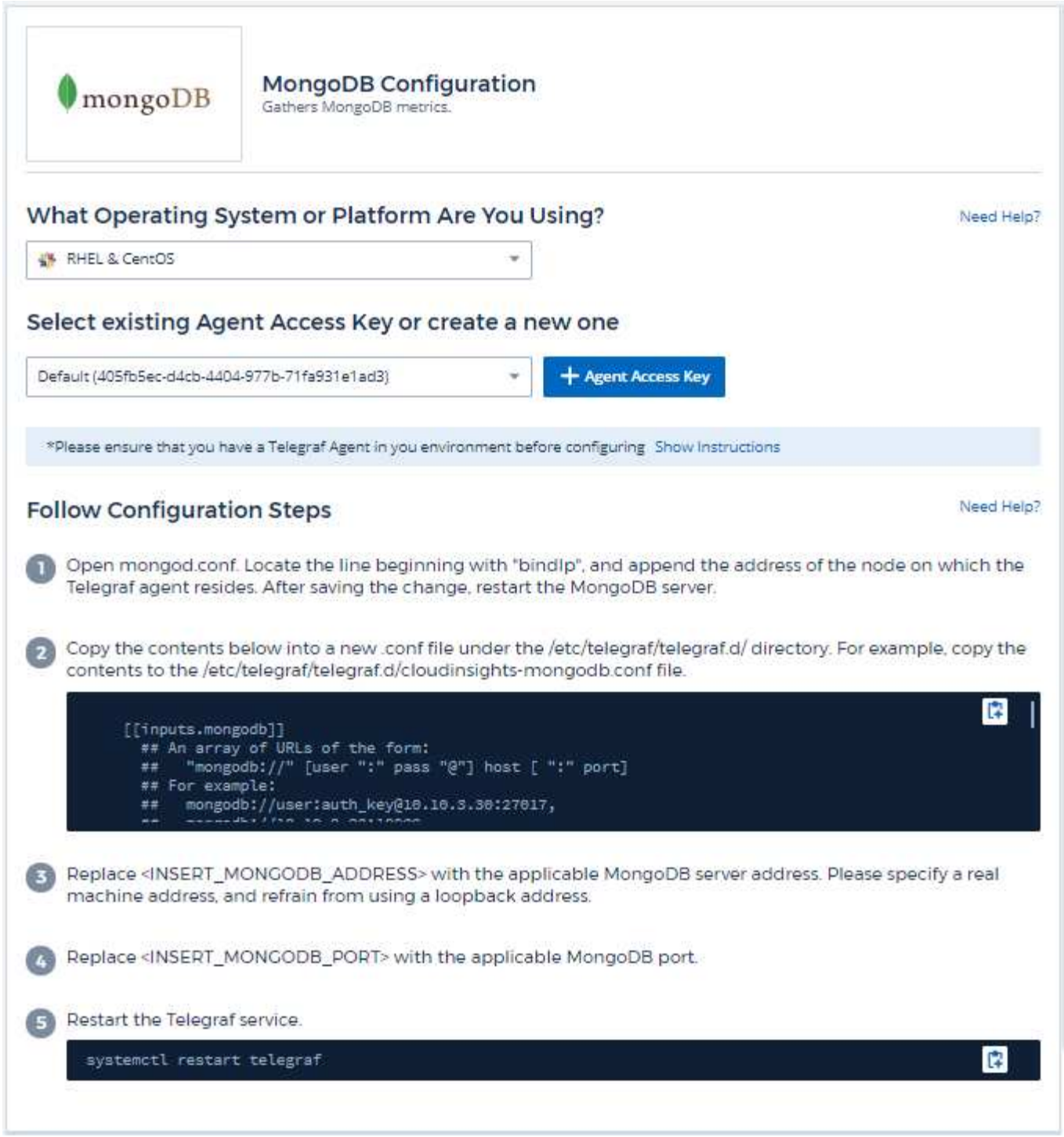
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da MongoDB.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli MongoDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione MongoDB" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
MongoDB	Nome host dello spazio dei nomi		
Database MongoDB	Nome host dello spazio dei nomi Nome del database		

Risoluzione dei problemi

Le informazioni possono essere trovate da"Supporto" pagina.

Raccoglitore dati MySQL

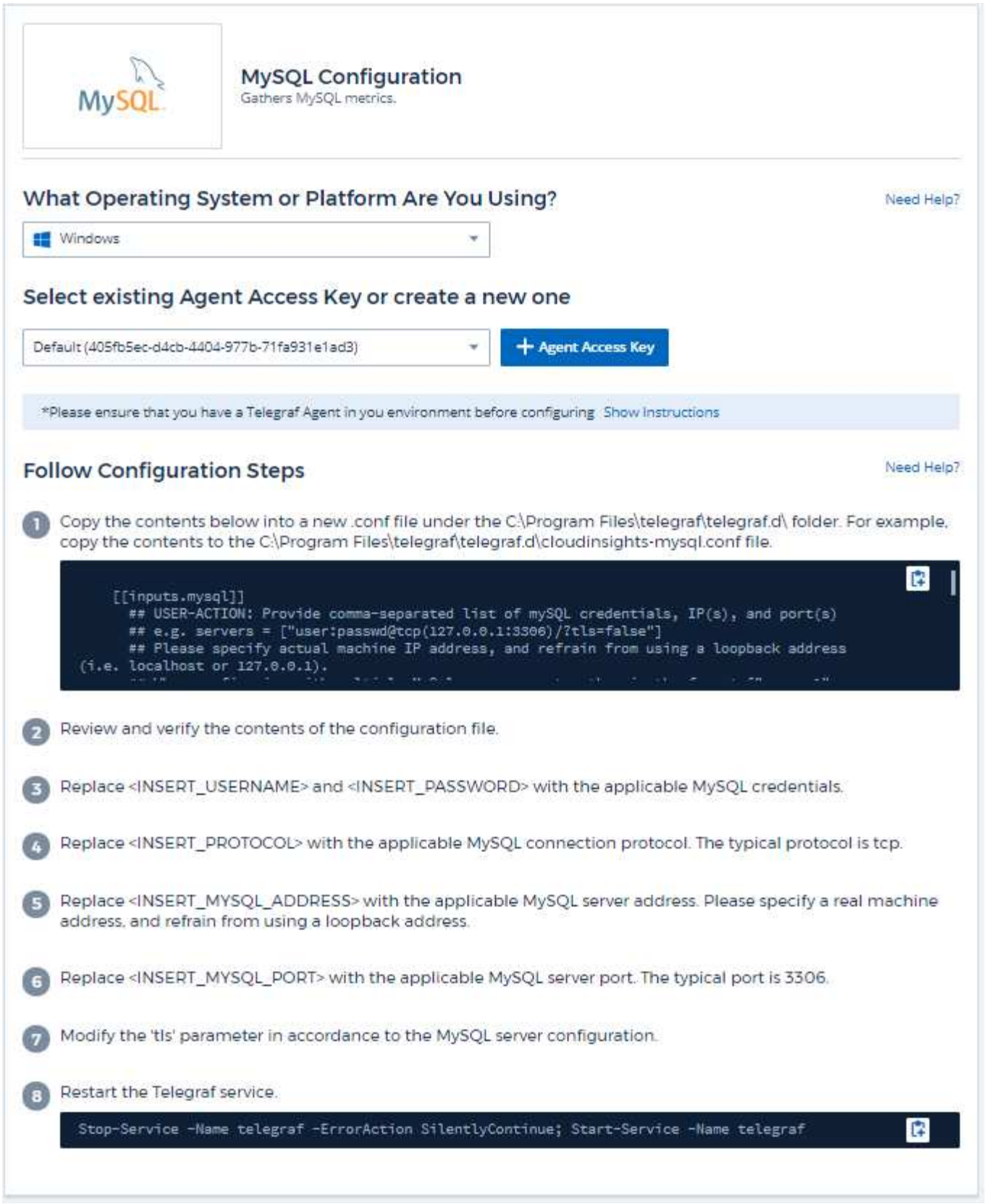
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da MySQL.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli MySQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione MySQL" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
MySQL	Spazio dei nomi MySQL Server	IP del nodo Nome del nodo	Client interrotti (al secondo) Connessioni interrotte (al secondo) Byte RX (al secondo) Byte TX (al secondo) Comandi Admin (al secondo) Comandi Comandi Alter Event Comandi Alter Function Comandi Alter Instance Comandi Alter Procedure Comandi Alter Server Comandi Alter Table Comandi Alter Tablespace Comandi Alter User Comandi Analyze Comandi Assign To Keycache Comandi Begin Comandi Binlog Comandi Call Procedure Comandi Change DB Comandi Change Master Comandi Change Repl Filter Comandi Check Comandi Checksum Comandi Commit Comandi Create DB Comandi Create Event Comandi Create Function Comandi Create Index Comandi Create Procedure Comandi Create Server Comandi Create Table Comandi Create Trigger Comandi Create UDF Comandi Create User Comandi Create View Errori di connessione SQL Dealloc Accetta tabelle disco Tmp create Errori ritardati Comandi Flush Gestore Commit Byte del buffer pool Innodb Blocchi chiave dati non svuotati Richieste di lettura chiave Richieste di scrittura chiave Scritture chiave Tempo massimo di esecuzione Superato il numero massimo di connessioni utilizzate File aperti Prestazioni Schema Account persi Conteggio stmt preparati Qcache Blocchi liberi Query Domande Seleziona

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati Netstat

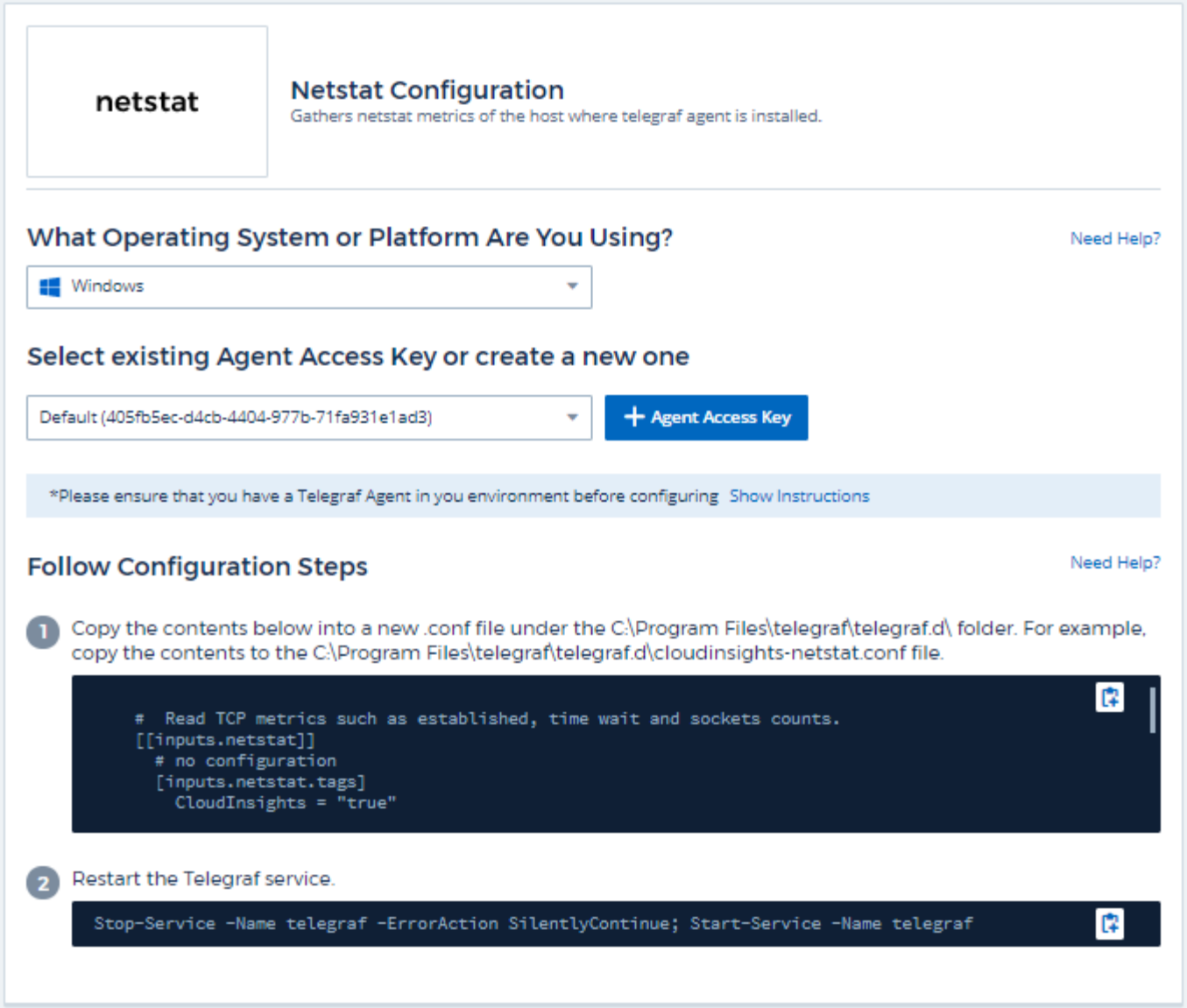
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere le metriche Netstat.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Selezionare Netstat.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Netstat	Nodo UUID	IP del nodo Nome del nodo	

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati Nginx

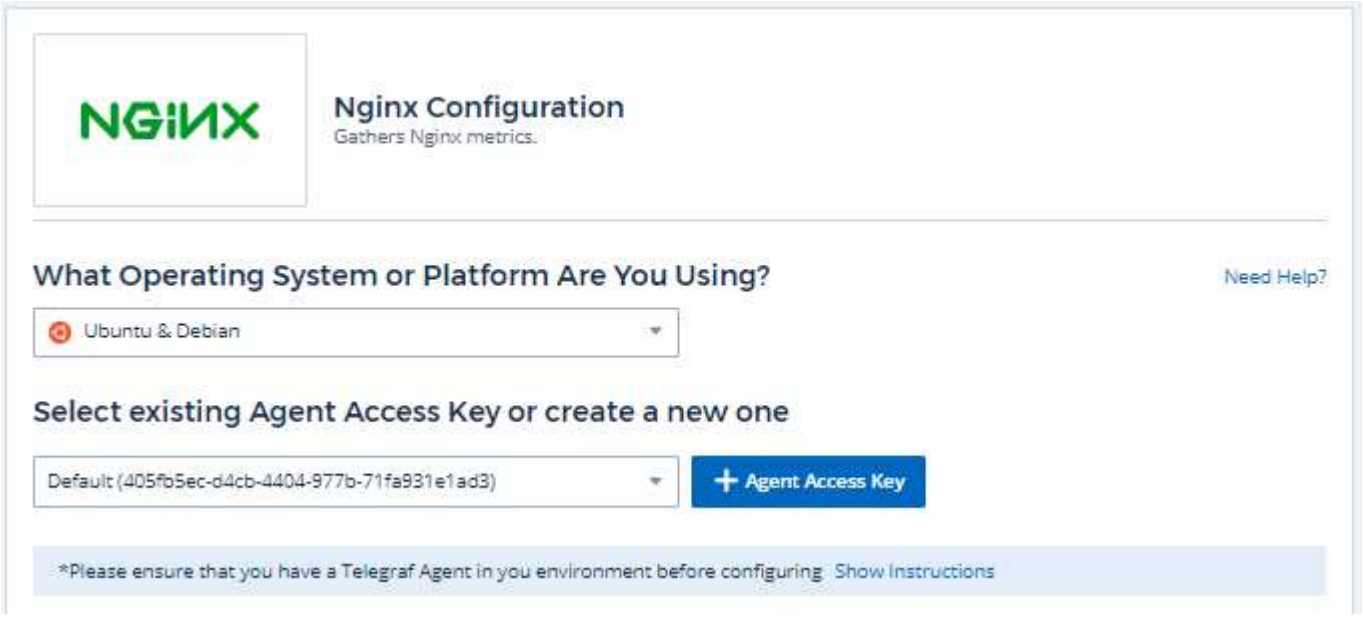
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Nginx.

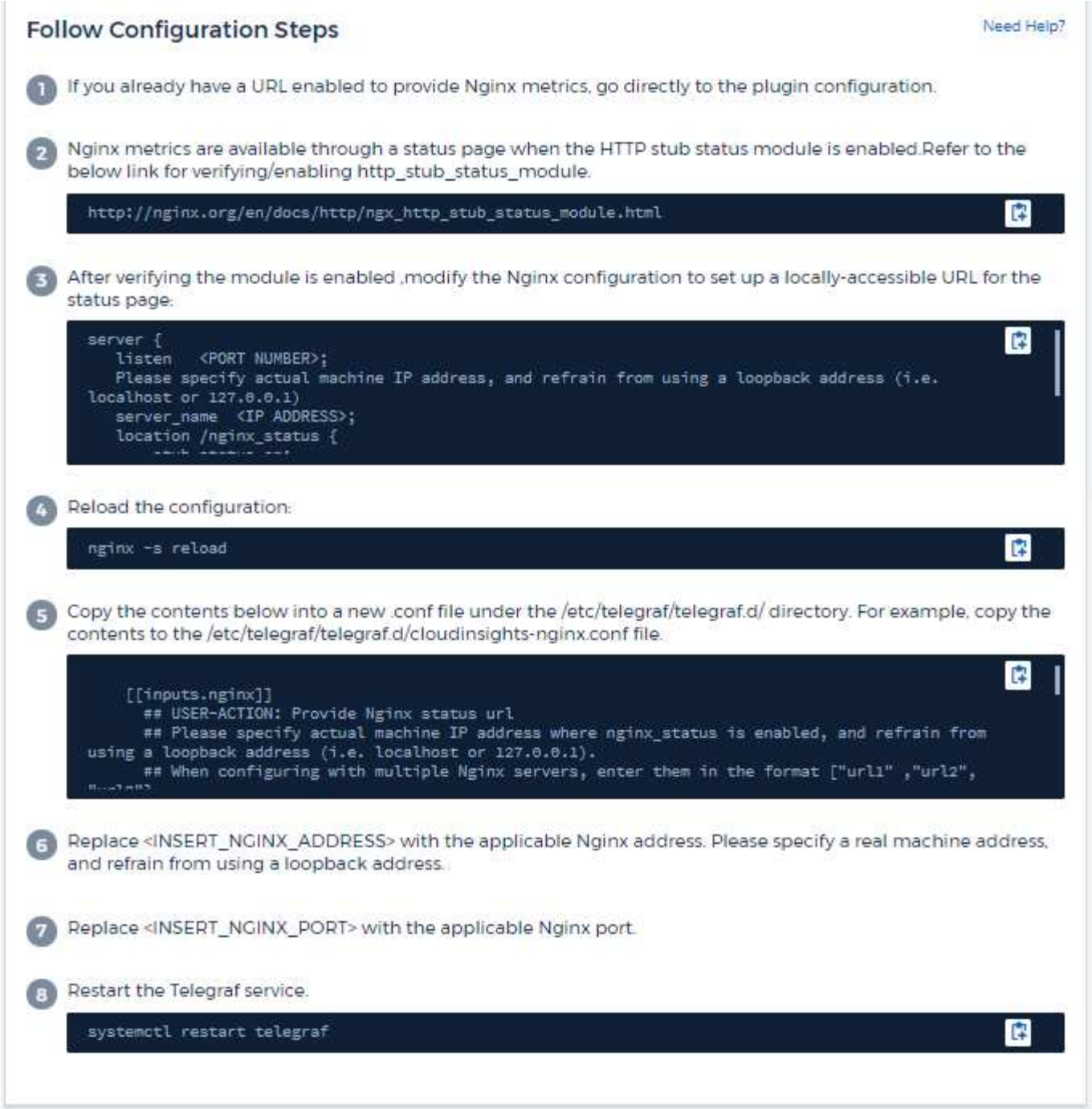
Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Nginx.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.





Impostare

La raccolta delle metriche Nginx richiede che Nginx"http_stub_status_module" essere abilitato.

Ulteriori informazioni possono essere trovate nel"Documentazione Nginx" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nginx	Server dello spazio dei nomi	IP del nodo Nome del nodo Porta	Accetta richieste di lettura gestite attive in attesa di scrittura

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati PostgreSQL

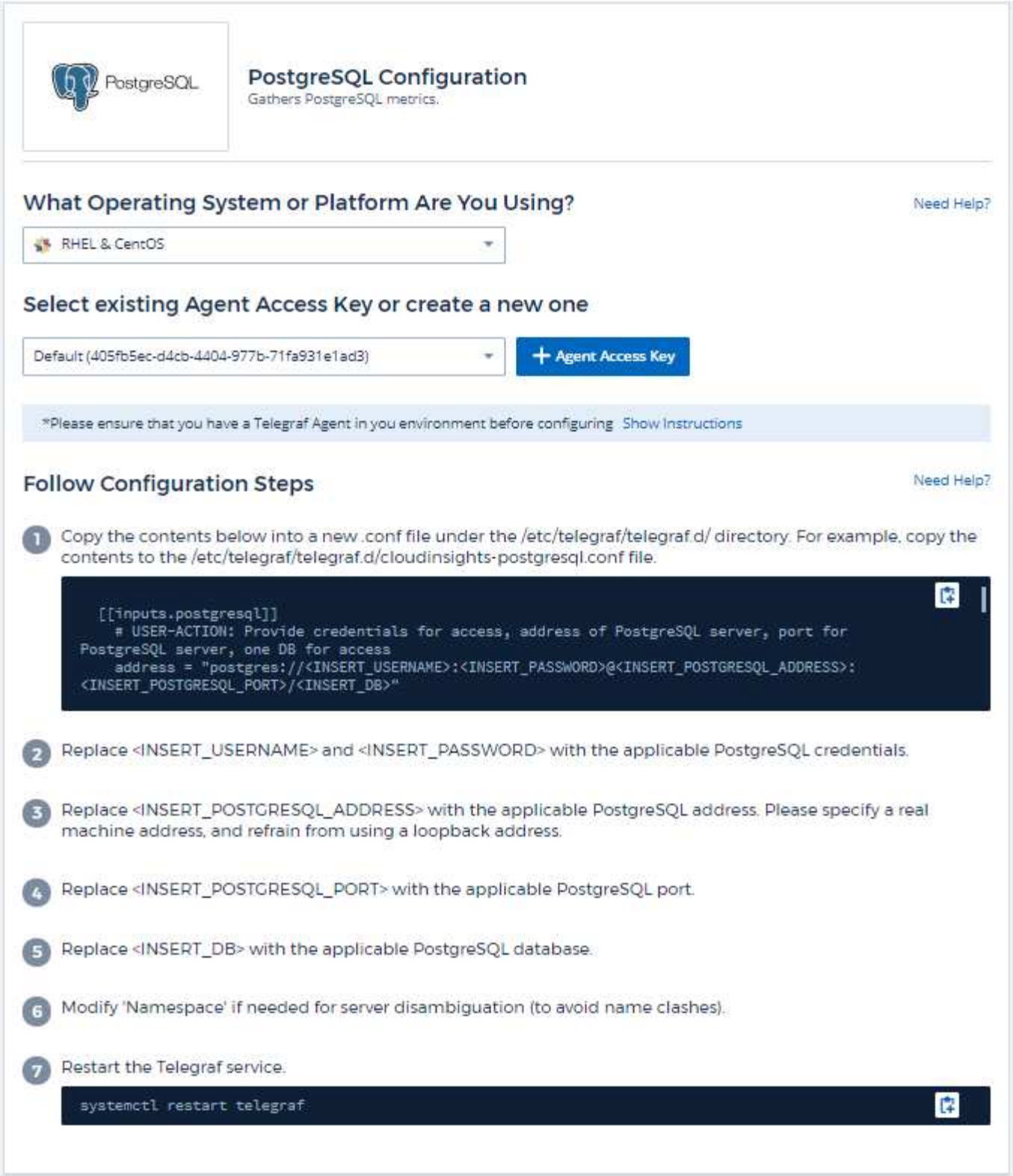
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da PostgreSQL.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli PostgreSQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione PostgreSQL" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server PostgreSQL	Server di database dello spazio dei nomi	Nome nodo IP nodo	Buffer allocati Buffer backend Buffer di sincronizzazione file backend Buffer di checkpoint Checkpoint puliti Checkpoint di tempo di sincronizzazione Checkpoint di tempo di scrittura Richieste Checkpoint Tempo massimo di scrittura pulita
Database PostgreSQL	Server di database dello spazio dei nomi	OID del database Nome del nodo IP del nodo	Blocchi Tempo di lettura Blocchi Tempo di scrittura Blocchi Hit Blocchi Letture Conflitti Deadlock Numero client File temporanei Byte Numero file temporanei Righe Righe eliminate Righe recuperate Righe inserite Righe restituite Transazioni aggiornate Transazioni confermate Rollback

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore di dati dell'agente fantoccio

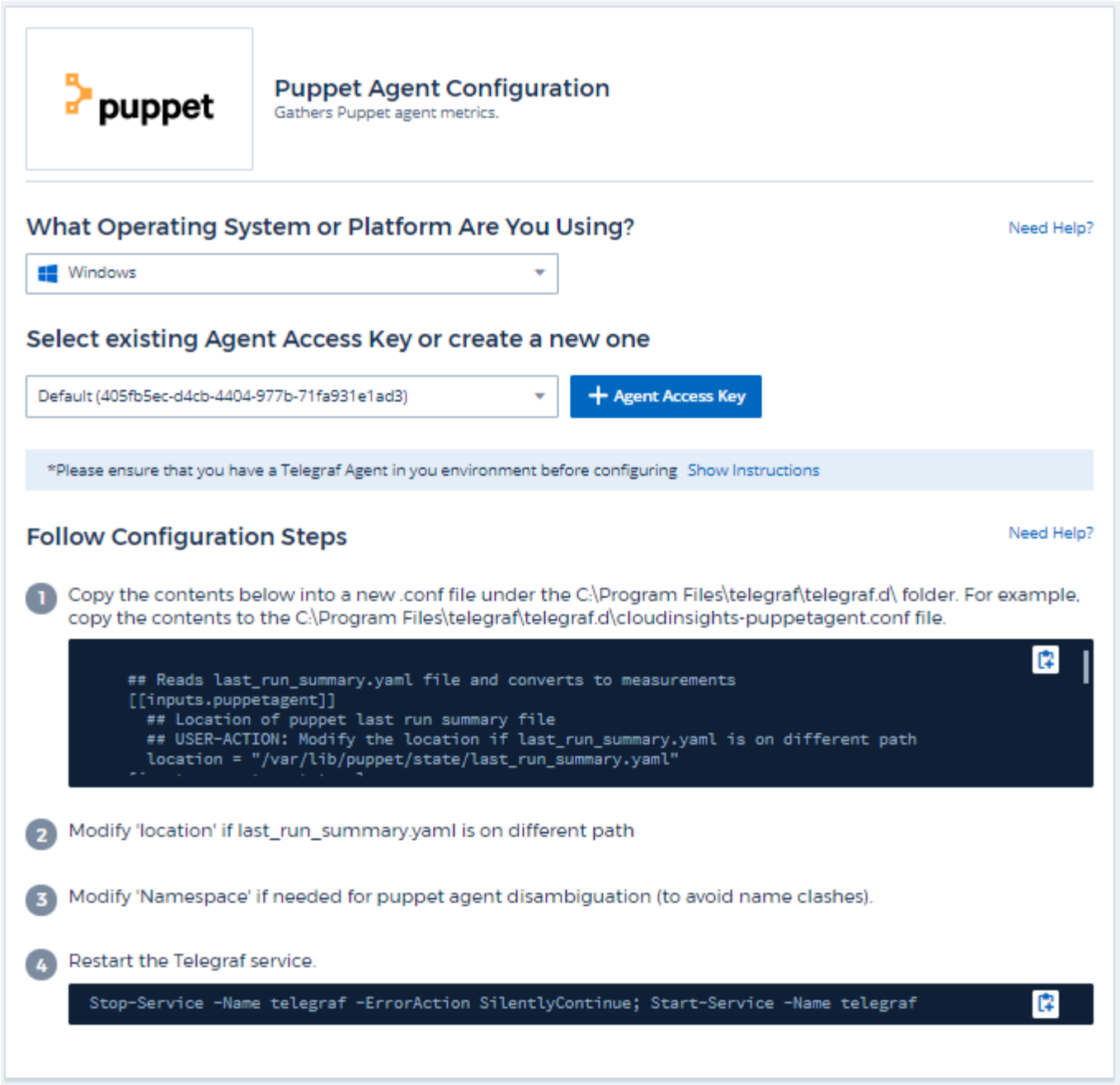
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Puppet Agent.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Marionetta.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel "Documentazione dei burattini"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:

Agente burattino	UUID del nodo dello spazio dei nomi	Nome nodo Posizione IP nodo Versione Configstring Versione Puppet	Modifiche Eventi totali Eventi di errore Eventi di successo Risorse totali Risorse modificate Risorse non riuscite Risorse non riavviate Risorse non sincronizzate Risorse riavviate Risorse pianificate Risorse ignorate Tempo totale Tempo di ancoraggio Tempo di configretrieval Tempo di cron Tempo di esecuzione Tempo di file Tempo di filebucket Tempo di ultima esecuzione Tempo del pacchetto Tempo di pianificazione Tempo di servizio Tempo di sshauthorizedkey Tempo totale utente

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Redis Data Collector

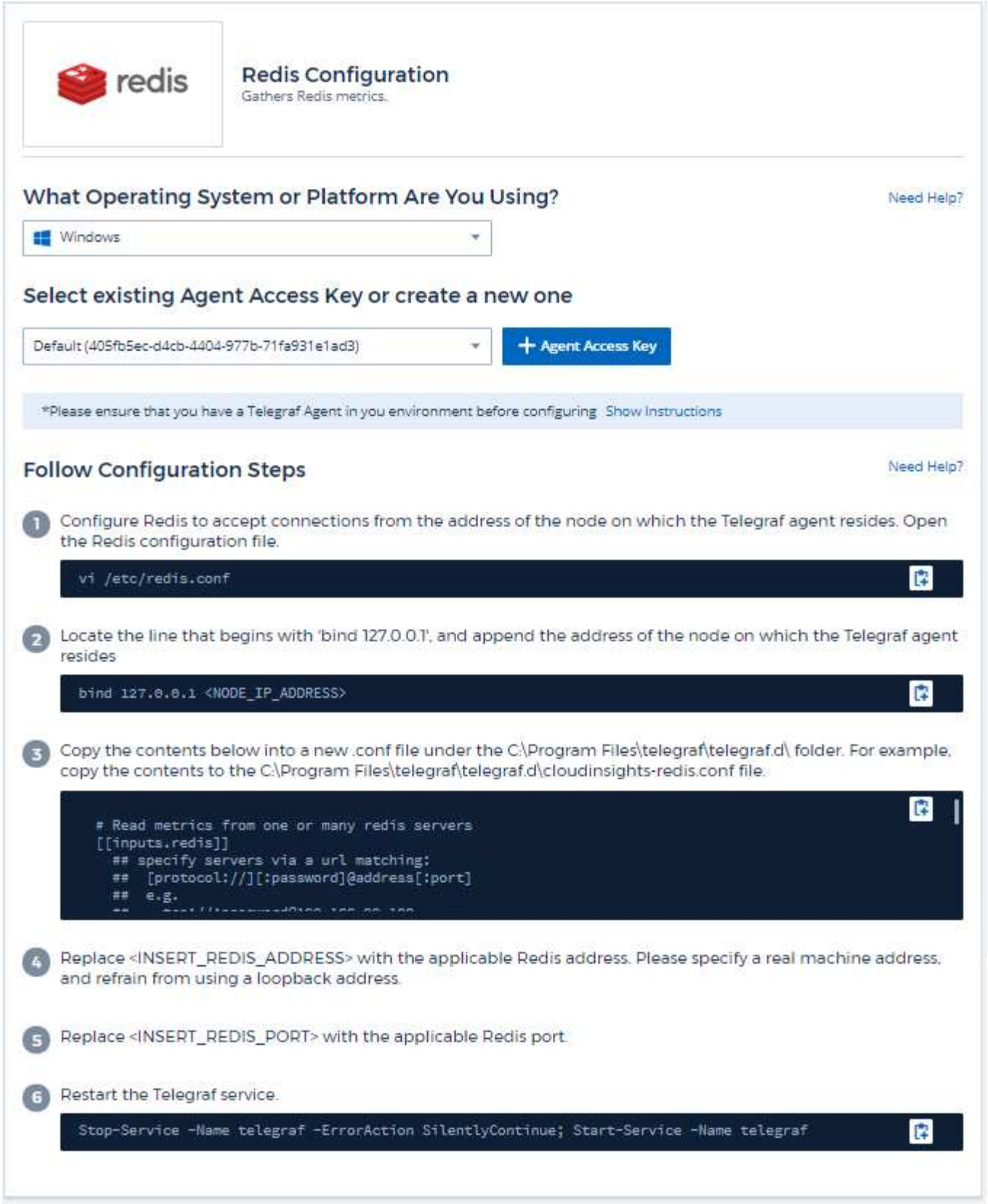
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Redis. Redis è un archivio di strutture dati in memoria open source utilizzato come database, cache e broker di messaggi, che supporta le seguenti strutture dati: stringhe, hash, elenchi, set e altro ancora.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Redis.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione Redis" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Redis	Server dello spazio dei nomi		

Risoluzione dei problemi

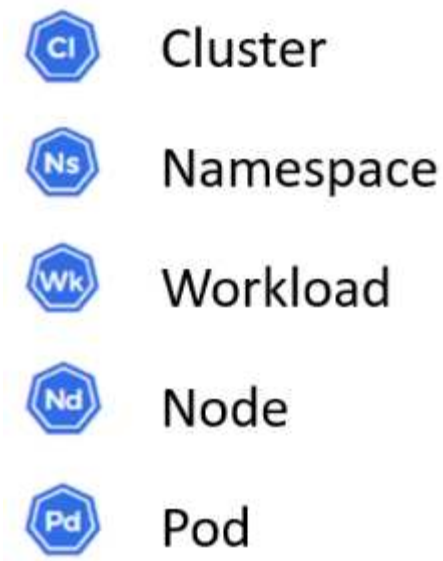
Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Riferimento alle icone degli oggetti

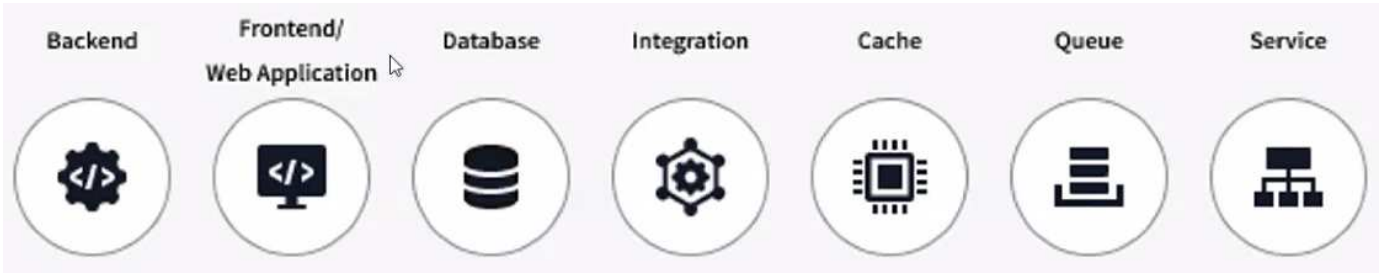
Icone degli oggetti utilizzate in Data Infrastructure Insights.

Icone dell'infrastruttura:

Icone di Kubernetes:



Icone di monitoraggio delle prestazioni di rete e mappa di Kubernetes:



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/"

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/"

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/"

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

Avviso per Data Infrastructure Insights (in precedenza Cloud Insights), window=_blank

Avviso per Workload Security (in precedenza Cloud Secure), window=_blank

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.