Documentazione Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
February 26, 2026

This PDF was generated from https://docs.netapp.com/it-it/storage-management-cloud-volumes-ontap/index.html on February 26, 2026. Always check docs.netapp.com for the latest.

Sommario

Documentazione Cloud Volumes ONTAP . . . 1
Note di rilascio . . . 2
Novità di Cloud Volumes ONTAP . . . 2
26 febbraio 2026 . . . 2
19 febbraio 2026 . . . 4
17 febbraio 2026 . . . 4
12 febbraio 2026 . . . 5
10 febbraio 2026 . . . 6
9 febbraio 2026 . . . 6
12 gennaio 2026 . . . 8
10 dicembre 2025 . . . 8
10 novembre 2025 . . . 9
17 ottobre 2025 . . . 9
06 ottobre 2025 . . . 9
04 settembre 2025 . . . 10
11 agosto 2025 . . . 10
14 luglio 2025 . . . 10
25 giugno 2025 . . . 11
29 maggio 2025 . . . 11
12 maggio 2025 . . . 11
16 aprile 2025 . . . 11
14 aprile 2025 . . . 12
03 aprile 2025 . . . 12
28 marzo 2025 . . . 12
12 marzo 2025 . . . 12
10 marzo 2025 . . . 12
06 marzo 2025 . . . 13
03 marzo 2025 . . . 13
18 febbraio 2025 . . . 13
10 febbraio 2025 . . . 13
09 dicembre 2024 . . . 14
11 novembre 2024 . . . 14
25 ottobre 2024 . . . 15
07 ottobre 2024 . . . 16
09 settembre 2024 . . . 16
23 agosto 2024 . . . 16
22 agosto 2024 . . . 17
08 agosto 2024 . . . 17
10 giugno 2024 . . . 17
17 maggio 2024 . . . 17
23 aprile 2024 . . . 18
08 marzo 2024 . . . 18
05 marzo 2024 . . . 18

02 febbraio 2024 . . . 19
16 gennaio 2024 . . . 19
08 gennaio 2024 . . . 19
06 dicembre 2023 . . . 19
05 dicembre 2023 . . . 20
10 novembre 2023 . . . 20
08 novembre 2023 . . . 21
01 novembre 2023 . . . 21
23 ottobre 2023 . . . 21
06 ottobre 2023 . . . 21
10 settembre 2023 . . . 22
30 luglio 2023 . . . 22
26 luglio 2023 . . . 23
02 luglio 2023 . . . 23
26 giugno 2023 . . . 23
04 giugno 2023 . . . 23
07 maggio 2023 . . . 24
04 aprile 2023 . . . 24
3 aprile 2023 . . . 25
13 marzo 2023 . . . 27
05 marzo 2023 . . . 27
05 febbraio 2023 . . . 28
1 gennaio 2023 . . . 29
15 dicembre 2022 . . . 29
08 dicembre 2022 . . . 29
04 dicembre 2022 . . . 29
15 novembre 2022 . . . 30
06 novembre 2022 . . . 30
18 settembre 2022 . . . 30
31 luglio 2022 . . . 31
18 luglio 2022 . . . 32
3 luglio 2022 . . . 32
07 giugno 2022 . . . 33
02 maggio 2022 . . . 34
3 aprile 2022 . . . 36
27 febbraio 2022 . . . 36
09 febbraio 2022 . . . 37
06 febbraio 2022 . . . 37
30 gennaio 2022 . . . 37
02 gennaio 2022 . . . 38
28 novembre 2021 . . . 39
04 ottobre 2021 . . . 40
02 settembre 2021 . . . 40
07 luglio 2021 . . . 41
30 maggio 2021 . . . 43

24 maggio 2021 . . . 44
11 aprile 2021 . . . 44
08 marzo 2021 . . . 44
04 gennaio 2021 . . . 45
03 novembre 2020 . . . 47
Limitazioni note . . . 47
La console non supporta la creazione di volumi FlexGroup . . . 47
La console non supporta S3 con Cloud Volumes ONTAP . . . 47
La console non supporta il ripristino di emergenza per le VM di archiviazione . . . 47
Note sulla versione Cloud Volumes ONTAP . . . 48
Iniziare . . . 49
Scopri di più su Cloud Volumes ONTAP . . . 49
Versioni ONTAP supportate per le distribuzioni Cloud Volumes ONTAP . . . 50
AWS . . . 50
Azzurro . . . 51
Google Cloud . . . 51
Inizia ad usare Amazon Web Services . . . 52
Avvio rapido per Cloud Volumes ONTAP in AWS . . . 53
Pianifica la configurazione Cloud Volumes ONTAP in AWS . . . 54
Configura la tua rete . . . 58
Configura Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in AWS . . . 83
Imposta i ruoli AWS IAM per i nodi Cloud Volumes ONTAP . . . 86
Impostare le licenze per Cloud Volumes ONTAP in AWS . . . 95
Distribuisci Cloud Volumes ONTAP in AWS utilizzando la distribuzione rapida . . . 103
Avvia Cloud Volumes ONTAP in AWS . . . 106
Distribuisci Cloud Volumes ONTAP in AWS Secret Cloud o AWS Top Secret Cloud . . . 120
Inizia a usare Microsoft Azure . . . 136
Scopri le opzioni di distribuzione di Cloud Volumes ONTAP in Azure . . . 136
Inizia con NetApp Console . . . 137
Distribuisci Cloud Volumes ONTAP dal marketplace di Azure . . . 189
Inizia a usare Google Cloud . . . 193
Avvio rapido per Cloud Volumes ONTAP in Google Cloud . . . 193
Pianifica la configurazione Cloud Volumes ONTAP in Google Cloud . . . 194
Configurare la rete Google Cloud per Cloud Volumes ONTAP . . . 198
Configurare i controlli del servizio VPC per distribuire Cloud Volumes ONTAP in Google Cloud . . . 211
Crea un account di servizio Google Cloud per Cloud Volumes ONTAP . . . 213
Utilizzo di chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP . . . 216
Impostare le licenze per Cloud Volumes ONTAP in Google Cloud . . . 217
Avvia Cloud Volumes ONTAP in Google Cloud . . . 222
Verifica delle immagini di Google Cloud Platform . . . 235
Utilizzare Cloud Volumes ONTAP . . . 247
Gestione delle licenze . . . 247
Gestisci le licenze basate sulla capacità per Cloud Volumes ONTAP . . . 247
Gestisci gli abbonamenti Keystone per Cloud Volumes ONTAP tramite NetApp Console . . . 252
Gestisci le licenze basate sui nodi per Cloud Volumes ONTAP . . . 254

Amministrazione del volume e LUN . . . 259
Creare un FlexVol volume su un sistema Cloud Volumes ONTAP . . . 259
Gestisci i volumi sui sistemi Cloud Volumes ONTAP . . . 266
Trasferisci i dati Cloud Volumes ONTAP inattivi in un archivio di oggetti a basso costo . . . 275
Connettiti a un LUN su Cloud Volumes ONTAP dal tuo sistema host . . . 283
Accelera l'accesso ai dati con i volumi FlexCache su un sistema Cloud Volumes ONTAP . . . 284
Amministrazione aggregata . . . 286
Creare un aggregato per i sistemi Cloud Volumes ONTAP . . . 286
Gestisci gli aggregati per i cluster Cloud Volumes ONTAP . . . 288
Gestire la capacità aggregata di Cloud Volumes ONTAP su un agente Console . . . 289
Gestire le prestazioni del disco in Azure . . . 291
Amministrazione della VM di archiviazione . . . 294
Gestisci le VM di archiviazione per Cloud Volumes ONTAP . . . 294
Gestisci le VM di archiviazione dati per Cloud Volumes ONTAP in AWS . . . 296
Gestisci le VM di archiviazione per il servizio dati per Cloud Volumes ONTAP in Azure . . . 303
Gestisci le VM di archiviazione dati per Cloud Volumes ONTAP in Google Cloud . . . 306
Configurare il disaster recovery della VM di archiviazione per Cloud Volumes ONTAP . . . 309
Sicurezza e crittografia dei dati . . . 309
Crittografa i volumi su Cloud Volumes ONTAP con le soluzioni di crittografia NetApp . . . 309
Gestisci le chiavi di crittografia Cloud Volumes ONTAP con AWS Key Management Service . . . 310
Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Azure Key Vault . . . 311
Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Google Cloud KMS . . . 318
Abilita le soluzioni di protezione ransomware NetApp per Cloud Volumes ONTAP . . . 320
Crea copie Snapshot a prova di manomissione dei file WORM su Cloud Volumes ONTAP . . . 323
Amministrazione di sistema . . . 324
Aggiorna Cloud Volumes ONTAP . . . 324
Registra i sistemi Cloud Volumes ONTAP pay-as-you-go . . . 335
Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità . . . 336
Avviare e arrestare un sistema Cloud Volumes ONTAP . . . 339
Sincronizza l'ora di sistema Cloud Volumes ONTAP utilizzando il server NTP . . . 342
Modifica la velocità di scrittura del sistema . . . 342
Modificare la password di amministrazione del cluster Cloud Volumes ONTAP . . . 343
Aggiungere, rimuovere o eliminare sistemi . . . 344
Amministrazione AWS . . . 346
Amministrazione di Azure . . . 349
Amministrazione di Google Cloud . . . 361
Amministrare Cloud Volumes ONTAP utilizzando System Manager . . . 370
Amministra Cloud Volumes ONTAP dalla CLI . . . 372
Stato di salute e eventi del sistema . . . 373
Verifica la configurazione AutoSupport per Cloud Volumes ONTAP . . . 373
Configurare EMS per i sistemi Cloud Volumes ONTAP . . . 377
Concetti . . . 378
Licenza . . . 378
Licenze per Cloud Volumes ONTAP . . . 378
Scopri di più sulle licenze basate sulla capacità per Cloud Volumes ONTAP . . . 382

Magazzinaggio . . . 386
Protocolli client supportati per Cloud Volumes ONTAP . . . 386
Dischi e aggregati utilizzati per i cluster Cloud Volumes ONTAP . . . 387
Scopri di più sul supporto per AWS Elastic Volumes con Cloud Volumes ONTAP . . . 390
Scopri di più sulla suddivisione in livelli dei dati con Cloud Volumes ONTAP in AWS, Azure o Google Cloud . . . 396
Gestione dello storage Cloud Volumes ONTAP . . . 401
velocità di scrittura . . . 403
Cache flash . . . 406
Scopri di più sullo storage WORM su Cloud Volumes ONTAP . . . 407
Coppie ad alta disponibilità . . . 409
Scopri di più sulle coppie Cloud Volumes ONTAP HA in AWS . . . 409
Scopri di più sulle coppie Cloud Volumes ONTAP HA in Azure . . . 416
Scopri di più sulle coppie Cloud Volumes ONTAP HA in Google Cloud . . . 422
Operazioni non disponibili quando un nodo nella coppia Cloud Volumes ONTAP HA è offline . . . 427
Scopri di più sulla crittografia dei dati e sulla protezione ransomware Cloud Volumes ONTAP . . . 428
Crittografia dei dati a riposo . . . 428
Scansione antivirus ONTAP . . . 430
Protezione dal ransomware . . . 430
Scopri di più sul monitoraggio delle prestazioni per i carichi di lavoro Cloud Volumes ONTAP . . . 431
Rapporti tecnici sulle prestazioni . . . 431
Prestazioni della CPU . . . 431
Gestione delle licenze per BYOL basato su nodi . . . 431
Licenze del sistema BYOL . . . 431
Gestione delle licenze per un nuovo sistema . . . 432
Scadenza della licenza . . . 432
Rinnovo della licenza . . . 432
Trasferimento della licenza a un nuovo sistema . . . 433
Scopri come AutoSupport e Digital Advisor vengono utilizzati per Cloud Volumes ONTAP . . . 433
Configurazioni predefinite supportate per Cloud Volumes ONTAP . . . 434
Configurazione predefinita . . . 434
Dischi interni per i dati di sistema . . . 436
Conoscenza e supporto . . . 439
Registrati per ricevere supporto . . . 439
Panoramica della registrazione del supporto . . . 439
Registra NetApp Console per il supporto NetApp . . . 439
Associare le credenziali NSS per il supporto Cloud Volumes ONTAP . . . 441
Ottieni aiuto . . . 443
Ottieni supporto per un servizio file di un provider cloud . . . 443
Utilizzare opzioni di auto-supporto . . . 443
Crea un caso con il supporto NetApp . . . 443
Gestisci i tuoi casi di supporto . . . 446
Note legali . . . 447
Copyright . . . 447
Marchi . . . 447

Brevetti 447
Politica sulla riservatezza 447
Open source 447

Documentazione Cloud Volumes ONTAP

Note di rilascio

Novità di Cloud Volumes ONTAP

Scopri le novità sulla gestione Cloud Volumes ONTAP nella NetApp Console.

I miglioramenti descritti in questa pagina sono specifici per la gestione di Cloud Volumes ONTAP tramite la Console. Per scoprire le novità del software Cloud Volumes ONTAP , "vai alle Note sulla versione Cloud Volumes ONTAP" .

26 febbraio 2026

Supporto per Google Infrastructure Manager per distribuzioni in modalità privata

Cloud Volumes ONTAP 9.16.1 e versioni successive ora supportano "Google Cloud Infrastructure Manager" (IM) invece di "Cloud Deployment Manager" (DM) per le nuove distribuzioni in modalità privata in Google Cloud. Google ritirerà Deployment Manager come servizio infrastrutturale nel prossimo futuro per il più avanzato Infrastructure Manager.

A partire dal 25 febbraio 2026, Cloud Volumes ONTAP utilizza Infrastructure Manager per le nuove ed esistenti distribuzioni in modalità privata. Questa tabella illustra i flussi di lavoro di base per te:

Scenario	Azione	Nuove API per l'agente	Nuove autorizzazioni per l'agente	Nuove API Google Cloud per Cloud Volumes ONTAP	Risorse di documentazione
Agente esistente e distribuzione esistente in modalità privata	Aggiorna all'ultima versione dell'agente NetApp Console scaricando il programma di installazione dal NetApp Support Site e poi installando manualmente l'agente sul tuo host, così che possa utilizzare le API di Infrastructure Manager. Successivamente, converti i sistemi Cloud Volumes ONTAP esistenti per utilizzare Infrastructure Manager.	• API di Cloud Infrastructure Manager • API delle quote cloud • API Cloud Build	Tutti i permessi elencati per la release Console su: • "8 dicembre 2025" • "09 febbraio 2026" • cloudbuild.workerpools.get • cloudbuild.workerpools.get	• https://cloudbuild.googleapis.com/v1 • https://www.googleapis.com/upload/storage/v1 • https://config.googleapis.com/v1	"Configurare distribuzioni Cloud Volumes ONTAP esistenti per Google Cloud Infrastructure Manager"

Scenario	Azione	Nuove API per l'agente	Nuove autorizzazioni per l'agente	Nuove API Google Cloud per Cloud Volumes ONTAP	Risorse di documentazione
Nuovo agente e nuova distribuzione	Crea un nuovo agente e distribuisci un nuovo sistema Cloud Volumes ONTAP in modalità privata.				• "Crea un agente Console da Google Cloud" • "Avvio rapido per le distribuzioni in modalità privata"

Nelle distribuzioni in modalità privata, sono necessarie alcune modifiche alla configurazione affinché Cloud Volumes ONTAP possa iniziare a utilizzare Infrastructure Manager. Fare riferimento a "Configurazione di Infrastructure Manager per distribuzioni in modalità privata".

Link correlati

- "NetApp Console Agent 4.2.0 Note sulla versione"
- "Autorizzazioni richieste per Google Cloud Infrastructure Manager"

19 febbraio 2026

Nuove regioni supportate in Azure

Ora puoi distribuire Cloud Volumes ONTAP 9.12.1 GA e versioni successive in zone di disponibilità singole e multiple in Azure nelle seguenti regioni. Ciò include il supporto sia per distribuzioni a nodo singolo che ad alta disponibilità (HA).

- Giappone occidentale (japanwest)
- Indonesia centrale (indonesiacentral)

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali in Azure" .

17 febbraio 2026

Cloud Volumes ONTAP supporto per le VM Google Cloud di nuova generazione

Con la versione 9.18.1, NetApp passa le nuove distribuzioni di Cloud Volumes ONTAP dalle VM N2 alle VM di nuova generazione Google Cloud serie C3 per un'esperienza più veloce e scalabile. Ora puoi sfruttare le VM della serie C3 durante la distribuzione di Cloud Volumes ONTAP 9.18.1 e versioni successive in Google Cloud. Le macchine della serie C3 offrono prestazioni migliorate e limiti di capacità più elevati grazie all'utilizzo di Google Virtual NIC (gVNIC) e dischi Hyperdisk Balanced che garantiscono prestazioni dinamiche per carichi di lavoro intensivi.

Per ora, Cloud Volumes ONTAP supporta la serie C3 solo nelle distribuzioni a nodo singolo.

Se il tuo sistema Cloud Volumes ONTAP esegue la versione 9.18.1 o successiva, i pacchetti preconfigurati che utilizzi per le distribuzioni semplificate a nodo singolo utilizzano automaticamente le VM C3, consentendoti di personalizzare i parametri IOPS e throughput in base alle esigenze del tuo carico di lavoro. Analogamente, durante la creazione di aggregati, puoi aggiungere dischi Hyperdisk Balanced per ottenere prestazioni e scalabilità migliori in Google Cloud. Inoltre, puoi selezionare le varianti LSSD delle macchine della serie C3 per il supporto predefinito di Flash Cache.

Non è possibile modificare il tipo di disco per le VM C3 quando si aggiungono volumi agli aggregati perché C3 supporta solo dischi Hyperdisk Balanced. Analogamente, quando si replica un sistema con tipi di VM N2 su una VM C3, il tipo di disco è impostato per impostazione predefinita su Hyperdisk Balanced.

"Configurazioni supportate per Cloud Volumes ONTAP in Google Cloud"

"Documenti Google: serie di macchine C3"

Sicurezza VNet per Cloud Volumes ONTAP in Azure

Cloud Volumes ONTAP 9.18.1 e versioni successive distribuite in zone di disponibilità singole e multiple di Azure supportano la crittografia Azure Virtual Network (VNet) come parte della strategia di sicurezza a più livelli per proteggere i dati in transito. Cloud Volumes ONTAP sfrutta il protocollo Datagram Transport Layer Security (DTLS) nativo di Azure per proteggere la comunicazione tra nodi ONTAP, interfacce di gestione e altri servizi Azure, prevenendo intercettazioni e accessi non autorizzati. Questa crittografia a livello di rete integra le protezioni integrate di ONTAP per l'archiviazione e i dati a riposo, offrendo la sicurezza end-to-end dei dati.

"Networking per la crittografia di Azure VNet"

12 febbraio 2026

Supporto per VM Ebdsv5 e E104ids_v5 in Azure

A partire da Cloud Volumes ONTAP 9.18.1, è possibile distribuire Ebdsv5 ed E104ids_v5 VM per distribuzioni e aggiornamenti a nodo singolo e a coppia HA.

Le VM Ebdsv5 della famiglia Eb di macchine virtuali di Azure sono ottimizzate per una maggiore performance dello storage remoto. È possibile utilizzare queste VM per carichi di lavoro aziendali ad alto consumo di memoria e con elevati volumi di I/O, come database relazionali, analisi in-memory e altre applicazioni business-critical complesse.

E104ids_v5 è un'istanza di macchina virtuale isolata che consente di gestire meglio le finestre di manutenzione programmata. Rispetto a E80ids_v4, offre un throughput e IOPS molto più elevati, oltre a migliori prestazioni di rete complessive.

"Configurazioni supportate per Cloud Volumes ONTAP in Azure"

"Documentazione Azure: serie Edsv5 sizes"

10 febbraio 2026

Cloud Volumes ONTAP 9.18.1 GA

Ora puoi utilizzare la NetApp Console per distribuire e gestire la versione General Availability (GA) di Cloud Volumes ONTAP 9.18.1 in AWS, Azure e Google Cloud.

"Scopri di più su questa versione di Cloud Volumes ONTAP" .

9 febbraio 2026

Supporto per Google Cloud Infrastructure Manager

Cloud Volumes ONTAP 9.16.1 e versioni successive ora supportano "Google Cloud Infrastructure Manager" (IM) invece di "Cloud Deployment Manager" (DM) per le nuove distribuzioni in Google Cloud. Google ritirerà Deployment Manager come servizio infrastrutturale nel prossimo futuro per il più avanzato Infrastructure Manager.

A partire dal 9 febbraio 2026, Cloud Volumes ONTAP utilizza Infrastructure Manager per le distribuzioni nuove ed esistenti. Questa tabella spiega alcuni flussi di lavoro per te:

Scenario	Azione	Nuove API per l'agente	Nuove autorizzazioni per l'agente	Nuove API Google Cloud per Cloud Volumes ONTAP	Risorse di documentazione
Agente esistente e distribuzione Cloud Volumes ONTAP esistente	Aggiungere nuove API e autorizzazioni all'agente esistente e convertire il sistema Cloud Volumes ONTAP esistente.	• API di Cloud Infrastructure Manager • API delle quote cloud	Tutti i permessi elencati per la release Console su: • "8 dicembre 2025" • "09 febbraio 2026"	https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1	"Configurare le distribuzioni Cloud Volumes ONTAP esistenti per Google Cloud Infrastructure Manager"

Scenario	Azione	Nuove API per l'agente	Nuove autorizzazioni per l'agente	Nuove API Google Cloud per Cloud Volumes ONTAP	Risorse di documentazione
Agente esistente e nuova distribuzione Cloud Volumes ONTAP	Aggiungere nuove API e autorizzazioni all'agente esistente e distribuire un nuovo sistema Cloud Volumes ONTAP.	• API di Cloud Infrastructure Manager • API delle quote cloud	Tutti i permessi elencati per la release Console su: • "8 dicembre 2025" • "09 febbraio 2026"	Tutti i passaggi per una nuova distribuzione	"Introduzione a Cloud Volumes ONTAP in Google Cloud"
Nuovo agente e nuova distribuzione	Crea un nuovo agente e distribuisci un nuovo sistema Cloud Volumes ONTAP.				• "Crea un agente Console da Google Cloud" • "Introduzione a Cloud Volumes ONTAP in Google Cloud"

Ora, distribuisci Cloud Volumes ONTAP per utilizzare automaticamente Infrastructure Manager o passa le tue distribuzioni esistenti in Deployment Manager a Infrastructure Manager eseguendo uno strumento di conversione. La conversione è un processo una tantum, dopo il quale i tuoi sistemi inizieranno a utilizzare Infrastructure Manager. Consulta "Configura le distribuzioni Cloud Volumes ONTAP esistenti per Google Cloud Infrastructure Manager" per le istruzioni sull'esecuzione dello strumento di conversione.

I sistemi Cloud Volumes ONTAP che utilizzano Infrastructure Manager utilizzano i bucket di Google Cloud

Storage per archiviare dati e record nella zona del primo deployment, in modo da archiviare i record di deployment, che vengono riutilizzati per i deployment successivi. Potresti incorrere in costi aggiuntivi per questi bucket, ma non modificare o eliminare i bucket o il loro contenuto:

- `gs://netapp-cvo-infrastructure-manager-<project id>`: per le versioni ONTAP e i modelli SVM Terraform utilizzati per le nuove distribuzioni di Cloud Volumes ONTAP. Al suo interno, il bucket `dm-to-im-convert` contiene i file Terraform di Cloud Volumes ONTAP.
- `<gcp project number>-<region>-blueprint-config`: per l'archiviazione degli artefatti Google Cloud Terraform.

Link correlati

- "Introduzione a Cloud Volumes ONTAP in Google Cloud"
- "NetApp Console Agent 4.2.0 Note sulla versione"
- "Autorizzazioni richieste per Google Cloud Infrastructure Manager"

12 gennaio 2026

Opzione di fatturazione preferita per Cloud Volumes ONTAP

Ora puoi selezionare un'opzione di fatturazione preferita per calcolare l'utilizzo e gli eccedenti Cloud Volumes ONTAP . Dal 25 giugno 2025, data di disponibilità limitata del modello di licenza Bring Your Own Licenses (BYOL), NetApp ha aggiunto metodi di addebito preferiti nella sezione **Licenze e abbonamenti** della NetApp Console. Puoi utilizzare l'abbonamento annuale al marketplace per la fatturazione e gli eccedenti oppure il modello BYOL esistente come opzione preferita. Ciò ti offre la flessibilità di scegliere il metodo di addebito più adatto alla strategia finanziaria e ai modelli di utilizzo della tua organizzazione.

"Preferenze di fatturazione e superamenti".

10 dicembre 2025

Possibilità di migliorare le prestazioni dei dischi Premium SSD v2 in Azure

Ora puoi migliorare le prestazioni di Premium SSD v2 Managed Disks in Azure modificando i parametri IOPS e velocità effettiva. Utilizzando questa funzionalità, puoi ottimizzare le prestazioni di archiviazione dei tuoi sistemi in base ai requisiti del carico di lavoro.

"Gestisci le prestazioni del disco Premium SSD v2 per Cloud Volumes ONTAP in Azure".

Semplificazione della tariffazione eccedente per le licenze Essentials

Per i contratti annuali/offerte private del marketplace Cloud Volumes ONTAP , i calcoli del sovrapprezzo per le licenze Essentials sono ora allineati con i pacchetti Bring Your Own License (BYOL). In precedenza, gli eccessi venivano fatturati in base alle tariffe orarie di mercato per l'esatto pacchetto Essentials. Ora, se il tuo contratto annuale sul marketplace include più pacchetti Essentials, la NetApp Console addebita i costi aggiuntivi per un pacchetto Essentials rispetto alla capacità disponibile di un pacchetto Essentials più costoso nel tuo abbonamento. Ciò semplifica i calcoli del sovrapprezzo per i pacchetti Essentials e garantisce una transizione graduale dalla licenza BYOL a un modello basato su abbonamento.

"Come vengono addebitati gli eccessi per le licenze Essentials"

Supporto per le serie di dimensioni Azure Edsv6

A partire da Cloud Volumes ONTAP 9.17.1, è possibile distribuire VM della serie Azure Edsv6 tramite la NetApp Console per le nuove istanze Cloud Volumes ONTAP . Cloud Volumes ONTAP 9.17.1 e versioni successive supporteranno solo le VM di seconda generazione per le nuove distribuzioni. Queste macchine di seconda generazione sono compatibili con le tecnologie più recenti, come Unified Extensible Firmware Interface (UEFI), sistemi Azure Boost e NVMe. Sono ideali per sistemi e applicazioni ad alta intensità di memoria che necessitano di un'archiviazione locale veloce, come server di database e motori di analisi.

"Configurazioni supportate per Cloud Volumes ONTAP in Azure"

10 novembre 2025

Supporto NVMe-TCP migliorato

In precedenza, quando si distribuivano istanze Cloud Volumes ONTAP su NVMe-TCP, era necessario ottenere e applicare manualmente le licenze NVMe prima della distribuzione. Con questo aggiornamento, Cloud Volumes ONTAP ora installa automaticamente le licenze NVMe richieste durante la distribuzione, semplificando il processo di configurazione.

Per le distribuzioni NVMe-TCP esistenti prive di licenze, Cloud Volumes ONTAP applica le licenze automaticamente. È necessario riavviare il sistema affinché le licenze abbiano effetto.

Per maggiori informazioni, vedere "Protocolli client supportati per Cloud Volumes ONTAP: NVMe-TCP" .

17 ottobre 2025

Cloud Volumes ONTAP in Azure ora è limitato alle ultime versioni supportate

Le distribuzioni e gli aggiornamenti Cloud Volumes ONTAP in Azure tramite la NetApp Console sono ora limitati alle versioni più recenti supportate. Ciò garantisce la compatibilità con l'hardware di ultima generazione supportato da Microsoft e fornisce le funzionalità più recenti e i miglioramenti della sicurezza. La Console ti chiederà di effettuare l'aggiornamento alle versioni supportate.

Per maggiori dettagli, fare riferimento a:

- Distribuzione: "Versioni ONTAP supportate per le distribuzioni Cloud Volumes ONTAP"
- Aggiornamento: "Percorsi di aggiornamento supportati per Azure"

06 ottobre 2025

BlueXP è ora NetApp Console

NetApp Console, basata sulle fondamenta BlueXP migliorate e ristrutturate, offre una gestione centralizzata dello storage NetApp e NetApp Data Services in ambienti on-premise e cloud di livello aziendale, offrendo informazioni in tempo reale, flussi di lavoro più rapidi e un'amministrazione semplificata, il tutto in modo altamente sicuro e conforme.

Per i dettagli su cosa è cambiato, vedere il "Note sulla versione NetApp Console" .

Distribuzione semplificata Cloud Volumes ONTAP in AWS

Ora puoi distribuire Cloud Volumes ONTAP in AWS utilizzando un metodo di distribuzione rapido per configurazioni sia a nodo singolo che ad alta disponibilità (HA). Questo processo semplificato riduce il numero

di passaggi rispetto al metodo avanzato, imposta automaticamente i valori predefiniti in un'unica pagina e riduce al minimo la navigazione, rendendo la distribuzione più rapida e semplice.

Per ulteriori informazioni, consulta "Distribuisci Cloud Volumes ONTAP in AWS utilizzando la distribuzione rapida" .

04 settembre 2025

Cloud Volumes ONTAP 9.17.1 RC

Ora puoi utilizzare BlueXP per distribuire e gestire la Release Candidate 1 di Cloud Volumes ONTAP 9.17.1 in Azure e Google Cloud. Tuttavia, questa versione non è disponibile per la distribuzione e l'aggiornamento in AWS.

"Scopri di più su questa versione di Cloud Volumes ONTAP".

11 agosto 2025

Fine della disponibilità delle licenze ottimizzate

A partire dall'11 agosto 2025, la licenza Cloud Volumes ONTAP Optimized sarà deprecata e non sarà più disponibile per l'acquisto o il rinnovo nei marketplace di Azure e Google Cloud per gli abbonamenti con pagamento in base al consumo (PAYGO). Se hai un contratto annuale con una licenza Optimized, puoi continuare a utilizzare la licenza fino alla scadenza del contratto. Quando la licenza Optimized scade, puoi optare per le licenze Cloud Volumes ONTAP Essentials o Professional in BlueXP.

Tuttavia, la possibilità di aggiungere o rinnovare le licenze ottimizzate sarà disponibile tramite le API.

Per informazioni sui pacchetti di licenza, fare riferimento a "Licenze per Cloud Volumes ONTAP" .

Per informazioni sul passaggio a un metodo di ricarica diverso, fare riferimento a "Gestire le licenze basate sulla capacità" .

14 luglio 2025

Supporto per proxy trasparente

BlueXP ora supporta server proxy trasparenti oltre alle connessioni proxy esplicite esistenti. Durante la creazione o la modifica di BlueXP Connector, è possibile configurare un server proxy trasparente per gestire in modo sicuro il traffico di rete da e verso Cloud Volumes ONTAP.

Per ulteriori informazioni sull'utilizzo dei server proxy in Cloud Volumes ONTAP, fare riferimento a:

- "Configurazioni di rete per supportare il proxy del connettore in AWS"
- "Configurazioni di rete per supportare il proxy del connettore in Azure"
- "Configurazioni di rete per supportare il proxy del connettore in Google Cloud"

Nuovo tipo di VM supportato per Cloud Volumes ONTAP in Azure

A partire da Cloud Volumes ONTAP 9.13.1, L8s_v3 è supportato come tipo di VM nelle zone di disponibilità singole e multiple di Azure, sia per le distribuzioni di coppie ad alta disponibilità (HA) nuove che esistenti.

Per ulteriori informazioni, fare riferimento a "Configurazioni supportate in Azure" .

25 giugno 2025

Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP

A partire dal 25 giugno 2025, NetApp ha limitato il modello di licenza Bring Your Own License (BYOL) per Cloud Volumes ONTAP. La restrizione si applica a tutti i clienti e a tutte le distribuzioni Cloud Volumes ONTAP in AWS, Azure e Google Cloud. Le uniche eccezioni riguardano i clienti del settore pubblico statunitense e le distribuzioni nella regione Cina.

Il supporto e i servizi NetApp continueranno fino alla scadenza del contratto BYOL, ma le licenze scadute non verranno rinnovate né estese. Alla scadenza delle licenze BYOL, è necessario sostituirle con licenze basate sulla capacità acquistate tramite gli abbonamenti al marketplace cloud. Un modello di licenza basato sulla capacità, tramite i marketplace hyperscaler, semplifica l'esperienza di gestione delle licenze e offre maggiori vantaggi aziendali. Contatta il team Account NetApp o i rappresentanti del Customer Success per discutere le opzioni di conversione.

Per ulteriori informazioni, fare riferimento a questo comunicato clienti: "CPC-00661: Modifiche alla politica BYOL Cloud Volumes ONTAP" .

29 maggio 2025

Distribuzioni in modalità privata abilitate per Cloud Volumes ONTAP 9.15.1

Ora puoi distribuire Cloud Volumes ONTAP 9.15.1 in modalità privata su AWS, Azure e Google Cloud. La modalità privata è abilitata sia per le distribuzioni a nodo singolo che per quelle ad alta disponibilità (HA) di Cloud Volumes ONTAP 9.15.1.

Per ulteriori informazioni sulle distribuzioni in modalità privata, fare riferimento ahttps://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["Scopri di più sulle modalità di distribuzione di BlueXP"^] .

12 maggio 2025

Individuazione delle distribuzioni effettuate tramite Azure Marketplace in BlueXP

BlueXP è ora in grado di individuare i sistemi Cloud Volumes ONTAP distribuiti direttamente tramite Azure Marketplace. Ciò significa che ora è possibile aggiungere e gestire questi sistemi come ambienti di lavoro in BlueXP, proprio come qualsiasi altro sistema Cloud Volumes ONTAP .

"Distribuisci Cloud Volumes ONTAP dal marketplace di Azure"

16 aprile 2025

Nuove regioni supportate in Azure

Ora puoi distribuire Cloud Volumes ONTAP 9.12.1 GA e versioni successive in zone di disponibilità singole e multiple in Azure nelle seguenti regioni. Ciò include il supporto sia per distribuzioni a nodo singolo che ad alta disponibilità (HA).

- Spagna Centrale
- Messico Centrale

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali in Azure" .

14 aprile 2025

Creazione automatizzata di VM di archiviazione tramite le API in Google Cloud

Ora puoi utilizzare le API BlueXP per automatizzare la creazione di VM di archiviazione in Google Cloud. Hai utilizzato questa funzionalità nelle configurazioni ad alta disponibilità (HA) Cloud Volumes ONTAP e ora puoi utilizzarla anche nelle distribuzioni a nodo singolo. Utilizzando le API BlueXP , puoi facilmente creare, rinominare ed eliminare ulteriori VM di archiviazione dati nel tuo ambiente Google Cloud, senza dover configurare manualmente le interfacce di rete, i LIF e i LIF di gestione richiesti. Questa automazione semplifica il processo di gestione delle VM di archiviazione.

"Gestisci le VM di archiviazione dati per Cloud Volumes ONTAP in Google Cloud"

03 aprile 2025

Supporto per le regioni della Cina per Cloud Volumes ONTAP 9.13.1 in AWS

Ora puoi distribuire Cloud Volumes ONTAP 9.13.1 in AWS nelle regioni della Cina. Ciò include il supporto sia per distribuzioni a nodo singolo che ad alta disponibilità (HA). Sono supportate solo le licenze acquistate direttamente da NetApp .

Per la disponibilità regionale, fare riferimento a "Mappe delle regioni globali per Cloud Volumes ONTAP" .

28 marzo 2025

Distribuzioni in modalità privata abilitate per Cloud Volumes ONTAP 9.14.1

Ora puoi distribuire Cloud Volumes ONTAP 9.14.1 in modalità privata su AWS, Azure e Google Cloud. La modalità privata è abilitata sia per le distribuzioni a nodo singolo che per quelle ad alta disponibilità (HA) di Cloud Volumes ONTAP 9.14.1.

Per ulteriori informazioni sulle distribuzioni in modalità privata, fare riferimento ahttps://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["Scopri di più sulle modalità di distribuzione di BlueXP"^] .

12 marzo 2025

Nuove regioni supportate per distribuzioni con più zone di disponibilità in Azure

Le seguenti regioni ora supportano distribuzioni HA con più zone di disponibilità in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Stati Uniti centrali
- Governo degli Stati Uniti Virginia (Regione del governo degli Stati Uniti - Virginia)

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali in Azure" .

10 marzo 2025

Creazione automatizzata di VM di archiviazione tramite le API in Azure

Ora puoi usare le API BlueXP per creare, rinominare ed eliminare VM di archiviazione dati aggiuntive per Cloud Volumes ONTAP in Azure. L'utilizzo delle API automatizza il processo di creazione della VM di

archiviazione, inclusa la configurazione delle interfacce di rete richieste, dei LIF e di un LIF di gestione, se è necessario utilizzare una VM di archiviazione per scopi di gestione.

"Gestisci le VM di archiviazione per il servizio dati per Cloud Volumes ONTAP in Azure"

06 marzo 2025

Cloud Volumes ONTAP 9.16.1 GA

Ora puoi utilizzare BlueXP per distribuire e gestire la versione General Availability Cloud Volumes ONTAP 9.16.1 in Azure e Google Cloud. Tuttavia, questa versione non è disponibile per la distribuzione e l'aggiornamento in AWS.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

03 marzo 2025

Supporto per la regione Nuova Zelanda settentrionale in Azure

La regione Nuova Zelanda settentrionale è ora supportata in Azure per le configurazioni a nodo singolo e ad alta disponibilità (HA) di Cloud Volumes ONTAP 9.12.1 GA e versioni successive. Si noti che il tipo di istanza Lsv3 non è supportato in questa regione.

Per un elenco di tutte le regioni supportate, fare riferimento a "Mappa delle regioni globali in Azure" .

18 febbraio 2025

Introduzione alla distribuzione diretta di Azure Marketplace

Ora puoi sfruttare la distribuzione diretta di Azure Marketplace per distribuire in modo semplice e rapido Cloud Volumes ONTAP direttamente da Azure Marketplace. Utilizzando questo metodo semplificato, puoi esplorare le funzionalità e le capacità principali di Cloud Volumes ONTAP nel tuo ambiente senza dover configurare BlueXP Connector o soddisfare altri criteri di onboarding richiesti per la distribuzione di Cloud Volumes ONTAP tramite BlueXP.

- "Scopri le opzioni di distribuzione di Cloud Volumes ONTAP in Azure"
- "Distribuisci Cloud Volumes ONTAP dal marketplace di Azure"

10 febbraio 2025

Autenticazione utente abilitata per l'accesso a System Manager da BlueXP

In qualità di amministratore BlueXP , ora puoi attivare l'autenticazione per gli utenti ONTAP che accedono a ONTAP System Manager da BlueXP. È possibile abilitare questa opzione modificando le impostazioni di BlueXP Connector. Questa opzione è disponibile per le modalità standard e privata.

"Amministrare Cloud Volumes ONTAP utilizzando System Manager" .

BlueXP Advanced View è stato rinominato System Manager

L'opzione per la gestione avanzata di Cloud Volumes ONTAP da BlueXP tramite ONTAP System Manager è stata rinominata da **Advanced View** a **System Manager**.

"Amministrare Cloud Volumes ONTAP utilizzando System Manager" .

Introduzione di un modo più semplice per gestire le licenze con il BlueXP digital wallet

Ora puoi sperimentare una gestione semplificata delle licenze Cloud Volumes ONTAP utilizzando punti di navigazione migliorati all'interno del BlueXP digital wallet:

- Accedi facilmente alle informazioni sulla licenza Cloud Volumes ONTAP tramite le schede **Amministrazione > Licenses and subscriptions > Panoramica/Licenze dirette**.
- Fare clic su **Visualizza** nel pannello Cloud Volume ONTAP nella scheda **Panoramica** per ottenere una panoramica completa delle licenze basate sulla capacità. Questa visualizzazione avanzata offre informazioni dettagliate sulle tue licenze e sui tuoi abbonamenti.
- Se preferisci l'interfaccia precedente, puoi fare clic sul pulsante **Passa alla visualizzazione legacy** per visualizzare i dettagli della licenza in base al tipo e modificare i metodi di addebito per le tue licenze.

"Gestire le licenze basate sulla capacità" .

09 dicembre 2024

Elenco delle VM supportate aggiornato per Azure per allinearlo alle best practice

Le famiglie di macchine DS_v2 ed Es_v3 non sono più disponibili per la selezione su BlueXP quando si distribuiscono nuove istanze di Cloud Volumes ONTAP in Azure. Queste famiglie saranno mantenute e supportate solo nei sistemi più vecchi ed esistenti. Le nuove distribuzioni di Cloud Volumes ONTAP sono supportate in Azure solo a partire dalla versione 9.12.1. Ti consigliamo di passare a Es_v4 o a qualsiasi altra serie compatibile con Cloud Volumes ONTAP 9.12.1 e versioni successive. Tuttavia, le macchine delle serie DS_v2 ed Es_v3 saranno disponibili per nuove distribuzioni effettuate tramite API.

"Configurazioni supportate in Azure"

11 novembre 2024

Fine della disponibilità delle licenze basate su nodi

NetApp ha pianificato la fine della disponibilità (EOA) e la fine del supporto (EOS) delle licenze basate sui nodi Cloud Volumes ONTAP . A partire dall'11 novembre 2024, la disponibilità limitata delle licenze basate sui nodi è terminata. Il supporto per le licenze basate sui nodi termina il 31 dicembre 2024. Dopo l'EOA delle licenze basate sui nodi, dovresti passare alle licenze basate sulla capacità utilizzando lo strumento di conversione delle licenze BlueXP .

Per impegni annuali o a lungo termine, NetApp consiglia di contattare il proprio rappresentante NetApp prima della data di EOA o della data di scadenza della licenza per assicurarsi che siano soddisfatti i prerequisiti per la transizione. Se non si dispone di un contratto a lungo termine per un nodo Cloud Volumes ONTAP e si esegue il sistema con un abbonamento on-demand pay-as-you-go (PAYGO), è importante pianificare la conversione prima della data di fine del supporto. Sia per i contratti a lungo termine che per gli abbonamenti PAYGO, puoi utilizzare lo strumento di conversione delle licenze BlueXP per una conversione senza interruzioni.

"Fine della disponibilità delle licenze basate sui nodi" "Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità"

Rimozione delle distribuzioni basate su nodi da BlueXP

L'opzione per distribuire sistemi Cloud Volumes ONTAP utilizzando licenze basate su nodi è obsoleta su BlueXP. Ad eccezione di alcuni casi particolari, non è possibile utilizzare licenze basate su nodi per le distribuzioni Cloud Volumes ONTAP per nessun provider cloud.

NetApp riconosce i seguenti requisiti di licenza univoci in conformità con gli obblighi contrattuali e le esigenze operative e continuerà a supportare le licenze basate su nodi in queste situazioni:

- Clienti del settore pubblico statunitense
- Distribuzioni in modalità privata
- Distribuzioni nella regione cinese di Cloud Volumes ONTAP in AWS
- Se hai una licenza BYOL (licenza BY-NODE) valida e non scaduta

"Fine della disponibilità delle licenze basate sui nodi"

Aggiunta di un livello freddo per i dati Cloud Volumes ONTAP nell'archiviazione BLOB di Azure

BlueXP ora consente di selezionare un livello freddo per archiviare i dati del livello di capacità inattivo nell'archiviazione BLOB di Azure. Aggiungendo il livello freddo ai livelli caldo e freddo esistenti, si ottiene un'opzione di stoccaggio più conveniente e una migliore efficienza dei costi.

"Livelli dei dati in Azure"

Opzione per limitare l'accesso pubblico all'account di archiviazione per Azure

Ora hai la possibilità di limitare l'accesso pubblico al tuo account di archiviazione per i sistemi Cloud Volumes ONTAP in Azure. Disabilitando l'accesso, puoi proteggere il tuo indirizzo IP privato dall'esposizione anche all'interno della stessa rete virtuale, qualora fosse necessario rispettare le policy di sicurezza della tua organizzazione. Questa opzione disabilita anche la suddivisione in livelli dei dati per i sistemi Cloud Volumes ONTAP ed è applicabile sia ai nodi singoli che alle coppie ad alta disponibilità.

"Regole del gruppo di sicurezza" .

Abilitazione WORM dopo la distribuzione di Cloud Volumes ONTAP

Ora è possibile attivare l'archiviazione WORM (Write Once, Read Many) su un sistema Cloud Volumes ONTAP esistente utilizzando BlueXP. Questa funzionalità offre la flessibilità di abilitare WORM su un ambiente di lavoro, anche se WORM non è stato abilitato su di esso durante la sua creazione. Una volta abilitato, non è possibile disabilitare WORM.

"Abilitazione di WORM su un ambiente di lavoro Cloud Volumes ONTAP"

25 ottobre 2024

Elenco delle VM supportate aggiornato per Google Cloud per allinearlo alle best practice

Le macchine della serie n1 non sono più disponibili per la selezione su BlueXP quando si distribuiscono nuove istanze di Cloud Volumes ONTAP in Google Cloud. Le macchine della serie n1 saranno mantenute e supportate solo nei sistemi più vecchi ed esistenti. Le nuove distribuzioni di Cloud Volumes ONTAP sono supportate in Google Cloud solo a partire dalla versione 9.8. Ti consigliamo di passare ai tipi di macchine della serie n2 compatibili con Cloud Volumes ONTAP 9.8 e versioni successive. Le macchine della serie n1, tuttavia, saranno disponibili per nuove distribuzioni eseguite tramite API.

"Configurazioni supportate in Google Cloud" .

Supporto delle zone locali per Amazon Web Services in modalità privata

BlueXP ora supporta le distribuzioni ad alta disponibilità (HA) di AWS Local Zones for Cloud Volumes ONTAP in modalità privata. Il supporto che in precedenza era limitato alla sola modalità standard è stato ora esteso per includere la modalità privata.

Le zone locali AWS non sono supportate quando si utilizza BlueXP in modalità limitata.

Per ulteriori informazioni sulle zone locali AWS con distribuzioni HA, fare riferimento a"Zone locali AWS" .

07 ottobre 2024

Esperienza utente migliorata nella selezione della versione per l'aggiornamento

A partire da questa versione, quando si tenta di aggiornare Cloud Volumes ONTAP tramite la notifica BlueXP , si riceveranno indicazioni sulle versioni predefinite, più recenti e compatibili da utilizzare. Inoltre, ora puoi selezionare la patch più recente o la versione principale compatibile con la tua istanza Cloud Volumes ONTAP oppure inserire manualmente una versione per l'aggiornamento.

"Aggiorna il software Cloud Volumes ONTAP"

09 settembre 2024

Le funzionalità WORM e ARP non sono più a pagamento

Le funzionalità integrate di protezione dei dati e sicurezza WORM (Write Once Read Many) e ARP (Autonomous Ransomware Protection) saranno offerte con le licenze Cloud Volumes ONTAP senza costi aggiuntivi. Il nuovo modello di prezzo si applica sia agli abbonamenti BYOL e PAYGO/marketplace nuovi che a quelli esistenti di AWS, Azure e Google Cloud. Sia le licenze basate sulla capacità che quelle basate sui nodi conterranno ARP e WORM per tutte le configurazioni, comprese le coppie a nodo singolo e ad alta disponibilità (HA), senza costi aggiuntivi.

La tariffazione semplificata ti offre i seguenti vantaggi:

- Gli account che attualmente includono WORM e ARP non dovranno più sostenere costi per queste funzionalità. D'ora in poi, la fatturazione prevederà addebiti solo per l'utilizzo della capacità, come accadeva prima di questa modifica. WORM e ARP non saranno più inclusi nelle vostre fatture future.
- Se i tuoi account attuali non includono queste funzionalità, ora puoi optare per WORM e ARP senza costi aggiuntivi.
- Tutte le offerte Cloud Volumes ONTAP per tutti i nuovi account escluderanno i costi per WORM e ARP.

Scopri di più su queste funzionalità:

- "Abilita le soluzioni di protezione ransomware NetApp per Cloud Volumes ONTAP"
- "Deposito WORM"

23 agosto 2024

La regione Canada Ovest è ora supportata in AWS

La regione Canada Occidentale è ora supportata in AWS per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, vedere "Mappa delle regioni globali su AWS" .

22 agosto 2024

Cloud Volumes ONTAP 9.15.1 GA

BlueXP ora può distribuire e gestire la versione General Availability Cloud Volumes ONTAP 9.15.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

08 agosto 2024

I pacchetti di licenza di Edge Cache sono obsoleti

I pacchetti di licenze basati sulla capacità di Edge Cache non saranno più disponibili per le future distribuzioni di Cloud Volumes ONTAP. Tuttavia, è possibile utilizzare l'API per usufruire di questa funzionalità.

Supporto della versione minima per Flash Cache in Azure

La versione minima Cloud Volumes ONTAP richiesta per configurare Flash Cache in Azure è 9.13.1 GA. È possibile utilizzare solo ONTAP 9.13.1 GA e versioni successive per distribuire Flash Cache sui sistemi Cloud Volumes ONTAP in Azure.

Per le configurazioni supportate, vedere "Configurazioni supportate in Azure" .

Le prove gratuite per gli abbonamenti al marketplace sono deprecate

La licenza di prova gratuita o di valutazione automatica di 30 giorni per gli abbonamenti pay-as-you-go nel marketplace del provider cloud non sarà più disponibile in Cloud Volumes ONTAP. L'addebito per qualsiasi tipo di abbonamento al marketplace (PAYGO o contratto annuale) verrà attivato dal primo utilizzo, senza alcun periodo di prova gratuito.

10 giugno 2024

Cloud Volumes ONTAP 9.15.0

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.15.0 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

17 maggio 2024

Supporto per le zone locali di Amazon Web Services

Il supporto per AWS Local Zones è ora disponibile per le distribuzioni Cloud Volumes ONTAP HA. Le zone locali AWS sono un'implementazione dell'infrastruttura in cui storage, elaborazione, database e altri servizi AWS selezionati sono ubicati in prossimità di grandi città e aree industriali.

Le zone locali AWS sono supportate quando si utilizza BlueXP in modalità standard. Al momento, le zone locali AWS non sono supportate quando si utilizza BlueXP in modalità limitata o privata.

Per ulteriori informazioni sulle zone locali AWS con distribuzioni HA, fare riferimento a "Zone locali AWS" .

23 aprile 2024

Nuove regioni supportate per distribuzioni con più zone di disponibilità in Azure

Le seguenti regioni ora supportano distribuzioni HA con più zone di disponibilità in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Germania centro-occidentale
- Polonia Centrale
- Stati Uniti occidentali 3
- Israele Centrale
- Italia del Nord
- Canada Centrale

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali in Azure" .

La regione di Johannesburg è ora supportata in Google Cloud

La regione di Johannesburg(`africa-south1` regione) è ora supportato in Google Cloud per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali su Google Cloud" .

I modelli e i tag del volume non sono più supportati

Non è più possibile creare un volume da un modello o modificare i tag di un volume. Queste azioni erano associate al servizio di ripristino BlueXP , che non è più disponibile.

08 marzo 2024

Supporto per Amazon Instant Metadata Service v2

In AWS, Cloud Volumes ONTAP, Mediator e Connector ora supportano Amazon Instant Metadata Service v2 (IMDSv2) per tutte le funzioni. IMDSv2 offre una protezione avanzata contro le vulnerabilità. In precedenza era supportato solo IMDSv1.

Se richiesto dalle policy di sicurezza, è possibile configurare le istanze EC2 per utilizzare IMDSv2. Per le istruzioni, fare riferimento a "Documentazione di configurazione e amministrazione BlueXP per la gestione dei connettori esistenti" .

05 marzo 2024

Cloud Volumes ONTAP 9.14.1 GA

BlueXP ora può distribuire e gestire la versione di disponibilità generale Cloud Volumes ONTAP 9.14.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

02 febbraio 2024

Supporto per VM serie Edv5 in Azure

Cloud Volumes ONTAP supporta ora le seguenti VM della serie Edv5 a partire dalla versione 9.14.1.

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

"Configurazioni supportate in Azure"

16 gennaio 2024

Rilasci di patch in BlueXP

Le patch release sono disponibili in BlueXP solo per le ultime tre versioni di Cloud Volumes ONTAP.

"Aggiorna Cloud Volumes ONTAP"

08 gennaio 2024

Nuove VM per più zone di disponibilità di Azure

A partire da Cloud Volumes ONTAP 9.13.1, i seguenti tipi di VM supportano più zone di disponibilità di Azure per distribuzioni di coppie ad alta disponibilità nuove ed esistenti:

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Configurazioni supportate in Azure"

06 dicembre 2023

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.14.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

Limite massimo FlexVol volume di 300 TiB

Ora è possibile creare un FlexVol volume fino alla dimensione massima di 300 TiB con System Manager e ONTAP CLI a partire da Cloud Volumes ONTAP 9.12.1 P2 e 9.13.0 P2 e in BlueXP a partire da Cloud Volumes ONTAP 9.13.1.

- "Limiti di archiviazione in AWS"
- "Limiti di archiviazione in Azure"
- "Limiti di archiviazione in Google Cloud"

05 dicembre 2023

Sono state introdotte le seguenti modifiche.

Nuovo supporto regionale in Azure

Supporto per una singola zona di disponibilità

Le seguenti regioni ora supportano distribuzioni di zone di disponibilità singole ad alta disponibilità in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Tel Aviv
- Milano

Supporto per più regioni con zone di disponibilità

Le seguenti regioni ora supportano distribuzioni con più zone di disponibilità ad alta disponibilità in Azure per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- India centrale
- Norvegia orientale
- Svizzera del Nord
- Sud Africa del Nord
- Emirati Arabi Uniti del Nord

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali in Azure" .

10 novembre 2023

La seguente modifica è stata introdotta con la versione 3.9.35 del Connector.

La regione di Berlino ora è supportata in Google Cloud

La regione di Berlino è ora supportata in Google Cloud per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali su Google Cloud" .

08 novembre 2023

La seguente modifica è stata introdotta con la versione 3.9.35 del Connector.

La regione di Tel Aviv è ora supportata in AWS

La regione di Tel Aviv è ora supportata in AWS per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali su AWS" .

01 novembre 2023

La seguente modifica è stata introdotta con la versione 3.9.34 del Connector.

La regione dell'Arabia Saudita ora supportata in Google Cloud

La regione dell'Arabia Saudita è ora supportata in Google Cloud per Cloud Volumes ONTAP e Connector per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni, fare riferimento a "Mappa delle regioni globali su Google Cloud" .

23 ottobre 2023

La seguente modifica è stata introdotta con la versione 3.9.34 del Connector.

Nuove regioni supportate per distribuzioni HA con più zone di disponibilità in Azure

Le seguenti regioni di Azure ora supportano distribuzioni con più zone di disponibilità ad alta disponibilità per Cloud Volumes ONTAP 9.12.1 GA e versioni successive:

- Australia orientale
- Asia orientale
- Francia Centrale
- Nord Europa
- Qatar Centrale
- Svezia centrale
- Europa occidentale
- Stati Uniti occidentali 2

Per un elenco di tutte le regioni che supportano più zone di disponibilità, fare riferimento a "Mappa delle regioni globali in Azure" .

06 ottobre 2023

La seguente modifica è stata introdotta con la versione 3.9.34 del Connector.

Cloud Volumes ONTAP 9.14.0

BlueXP può ora distribuire e gestire la versione General Availability Cloud Volumes ONTAP 9.14.0 su AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

10 settembre 2023

La seguente modifica è stata introdotta con la versione 3.9.33 del Connector.

Supporto per VM serie Lsv3 in Azure

I tipi di istanza L48s_v3 e L64s_v3 sono ora supportati con Cloud Volumes ONTAP in Azure per distribuzioni a nodo singolo e a coppie ad alta disponibilità con dischi gestiti condivisi in zone di disponibilità singole e multiple, a partire dalla versione 9.13.1. Questi tipi di istanza supportano Flash Cache.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in Azure" "Visualizza i limiti di archiviazione per Cloud Volumes ONTAP in Azure"

30 luglio 2023

Con la versione 3.9.32 del Connector sono state introdotte le seguenti modifiche.

Supporto Flash Cache e alta velocità di scrittura in Google Cloud

La cache Flash e l'elevata velocità di scrittura possono essere abilitate separatamente in Google Cloud per Cloud Volumes ONTAP 9.13.1 e versioni successive. L'elevata velocità di scrittura è disponibile su tutti i tipi di istanza supportati. Flash Cache è supportato sui seguenti tipi di istanza:

- n2-standard-16
- n2-standard-32
- n2-standard-48
- n2-standard-64

È possibile utilizzare queste funzionalità separatamente o insieme sia nelle distribuzioni a nodo singolo che in quelle a coppia ad alta disponibilità.

"Avvia Cloud Volumes ONTAP in Google Cloud"

Miglioramenti dei report di utilizzo

Sono ora disponibili vari miglioramenti alle informazioni visualizzate nei report di utilizzo. Di seguito sono riportati i miglioramenti apportati ai report di utilizzo:

- L'unità TiB è ora inclusa nel nome delle colonne.
- È ora incluso un nuovo campo "nodo(i)" per i numeri di serie.
- Nel report sull'utilizzo delle VM di archiviazione è ora inclusa una nuova colonna "Tipo di carico di lavoro".
- I nomi degli ambienti di lavoro sono ora inclusi nei report sull'utilizzo dei volumi e delle VM di archiviazione.
- Il tipo di volume "file" è ora etichettato come "Primario (lettura/scrittura)".
- Il tipo di volume "secondario" è ora etichettato come "Secondario (DP)".

Per ulteriori informazioni sui report di utilizzo, fare riferimento a "Scarica i report di utilizzo" .

26 luglio 2023

Con la versione 3.9.31 del Connector sono state introdotte le seguenti modifiche.

Cloud Volumes ONTAP 9.13.1 GA

BlueXP può ora distribuire e gestire la versione General Availability Cloud Volumes ONTAP 9.13.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

02 luglio 2023

Con la versione 3.9.31 del Connector sono state introdotte le seguenti modifiche.

Supporto per distribuzioni HA con più zone di disponibilità in Azure

Japan East e Korea Central in Azure ora supportano distribuzioni HA con più zone di disponibilità per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Per un elenco di tutte le regioni che supportano più zone di disponibilità, fare riferimento a "Mappa delle regioni globali in Azure" .

Supporto per la protezione autonoma dal ransomware

La protezione autonoma contro i ransomware (ARP) è ora supportata su Cloud Volumes ONTAP. Il supporto ARP è disponibile su Cloud Volumes ONTAP versione 9.12.1 e successive.

Per saperne di più su ARP con Cloud Volumes ONTAP, fare riferimento a "Protezione autonoma dal ransomware" .

26 giugno 2023

La seguente modifica è stata introdotta con la versione 3.9.30 del Connector.

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.13.1 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

04 giugno 2023

La seguente modifica è stata introdotta con la versione 3.9.30 del Connector.

Aggiornamento del selettore della versione di aggiornamento Cloud Volumes ONTAP

Tramite la pagina Aggiorna Cloud Volumes ONTAP , ora puoi scegliere di eseguire l'aggiornamento all'ultima versione disponibile di Cloud Volumes ONTAP o a una versione precedente.

Per saperne di più sull'aggiornamento di Cloud Volumes ONTAP tramite BlueXP, fare riferimento a "Aggiorna Cloud Volumes ONTAP" .

07 maggio 2023

Con la versione 3.9.29 del Connector sono state introdotte le seguenti modifiche.

La regione del Qatar ora è supportata in Google Cloud

La regione del Qatar è ora supportata in Google Cloud per Cloud Volumes ONTAP e Connector per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

La regione Svezia Centrale è ora supportata in Azure

La regione Svezia Centrale è ora supportata in Azure per Cloud Volumes ONTAP e Connector for Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Supporto per distribuzioni HA con più zone di disponibilità in Azure Australia East

La regione Australia orientale in Azure ora supporta distribuzioni HA con più zone di disponibilità per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Ripartizione dell'utilizzo della ricarica

Ora puoi scoprire quanto ti viene addebitato quando sei abbonato a licenze basate sulla capacità. I seguenti tipi di report di utilizzo sono disponibili per il download dal portafoglio digitale in BlueXP. I report sull'utilizzo forniscono dettagli sulla capacità dei tuoi abbonamenti e ti indicano come ti vengono addebitate le risorse nei tuoi abbonamenti Cloud Volumes ONTAP . I report scaricabili possono essere facilmente condivisi con altri.

- Utilizzo del pacchetto Cloud Volumes ONTAP
- Utilizzo di alto livello
- Utilizzo delle VM di archiviazione
- Utilizzo dei volumi

Per ulteriori informazioni, consulta "Gestire le licenze basate sulla capacità" .

Ora viene visualizzata una notifica quando si accede a BlueXP senza un abbonamento al marketplace

Ora viene visualizzata una notifica ogni volta che si accede a Cloud Volumes ONTAP in BlueXP senza un abbonamento al marketplace. Nella notifica si legge che "è necessario un abbonamento al marketplace per questo ambiente di lavoro per essere conforme ai termini e alle condizioni Cloud Volumes ONTAP ".

Nuove autorizzazioni aggiunte alla policy AWS IAM per i mediatori HA

Queste nuove autorizzazioni AWS sono state aggiunte alla policy IAM per i mediatori HA negli ambienti ad alta disponibilità (HA) Cloud Volumes ONTAP :

- sts:AssumeRole
- ec2:Descrivi sottoreti

04 aprile 2023

Supporto per le regioni della Cina per AWS

A partire da Cloud Volumes ONTAP 9.12.1 GA, le regioni della Cina sono ora supportate in AWS come segue.

- Sono supportati i sistemi a nodo singolo.
- Sono supportate le licenze acquistate direttamente da NetApp .

Per la disponibilità regionale, fare riferimento a "Mappe delle regioni globali per Cloud Volumes ONTAP" .

3 aprile 2023

Con la versione 3.9.28 del Connector sono state introdotte le seguenti modifiche.

La regione di Torino ora supportata in Google Cloud

La regione di Torino è ora supportata in Google Cloud per Cloud Volumes ONTAP e Connector per Cloud Volumes ONTAP 9.12.1 GA e versioni successive.

Miglioramento BlueXP digital wallet

Il BlueXP digital wallet ora mostra la capacità concessa in licenza che hai acquistato con le offerte private del marketplace.

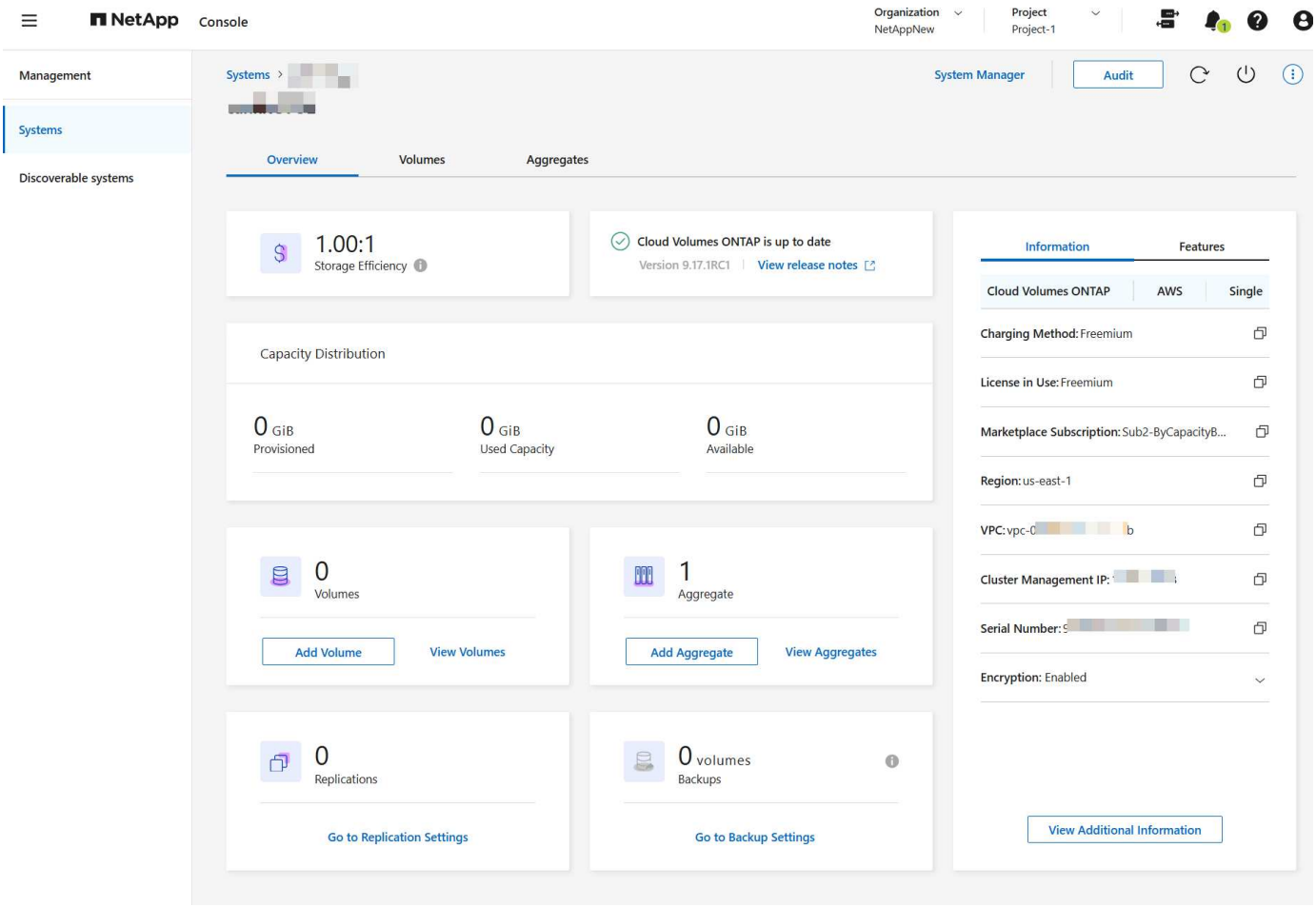
"Scopri come visualizzare la capacità consumata nel tuo account" .

Supporto per i commenti durante la creazione del volume

Questa versione consente di inserire commenti durante la creazione di un volume FlexGroup o FlexVol volume Cloud Volumes ONTAP quando si utilizza l'API.

Nuova progettazione dell'interfaccia utente BlueXP per le pagine Panoramica, Volumi e Aggregati Cloud Volumes ONTAP

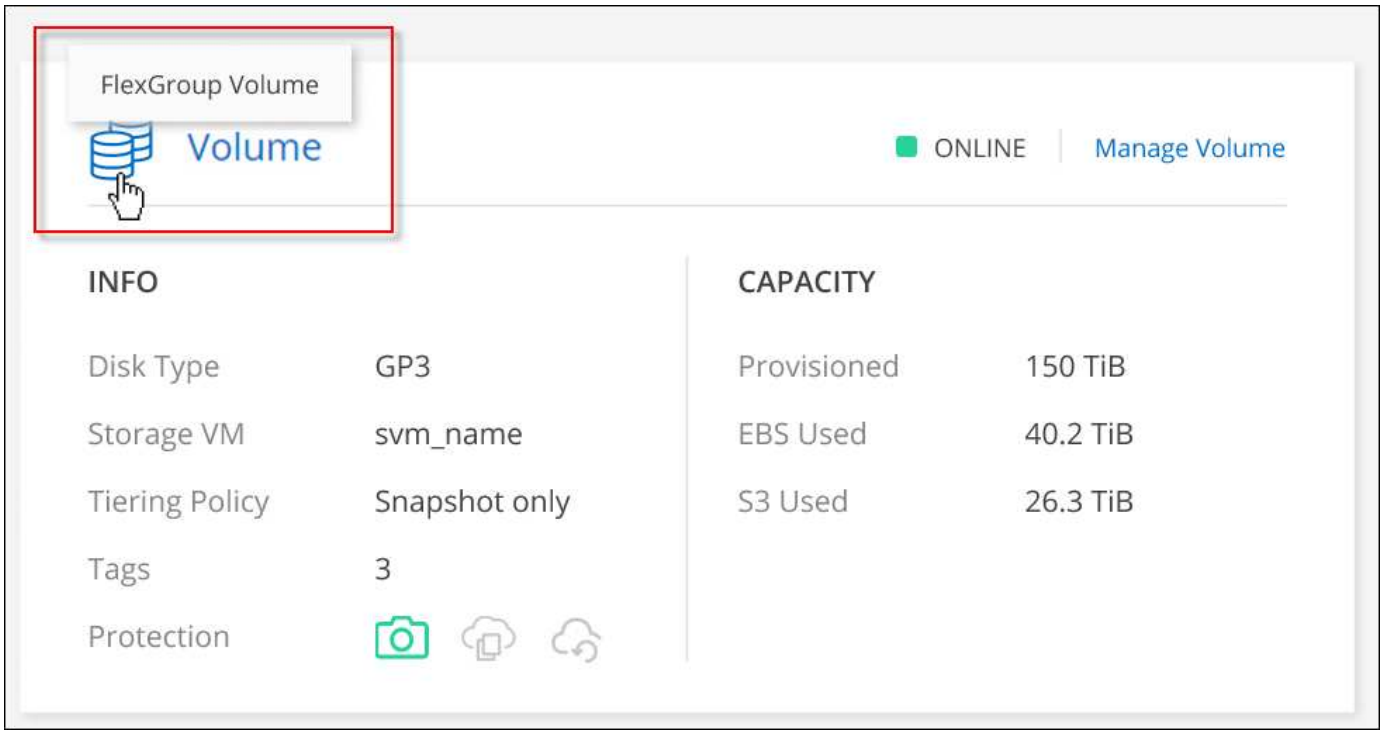
BlueXP ora ha un'interfaccia utente riprogettata per le pagine Panoramica, Volumi e Aggregati Cloud Volumes ONTAP . Il design basato su riquadri presenta informazioni più complete in ogni riquadro, per una migliore esperienza utente.



Volumi FlexGroup visualizzabili tramite Cloud Volumes ONTAP

I volumi FlexGroup creati direttamente tramite ONTAP System Manager o ONTAP CLI sono ora visualizzabili tramite il riquadro Volumi riprogettato in BlueXP. Analogamente alle informazioni fornite per i volumi FlexVol , BlueXP fornisce informazioni dettagliate per i volumi FlexGroup creati tramite un riquadro Volumi dedicato.

Attualmente è possibile visualizzare solo i volumi FlexGroup esistenti in BlueXP. La possibilità di creare volumi FlexGroup in BlueXP non è disponibile, ma è prevista per una versione futura.



"Scopri di più sulla visualizzazione dei volumi FlexGroup creati."

13 marzo 2023

Supporto per le regioni della Cina in Azure

La regione China North 3 è ora supportata per le distribuzioni a nodo singolo di Cloud Volumes ONTAP 9.12.1 GA e 9.13.0 GA in Azure. In queste regioni sono supportate solo le licenze acquistate direttamente da NetApp (licenze BYOL).

> Le nuove distribuzioni di Cloud Volumes ONTAP nelle regioni della Cina sono supportate solo nelle versioni 9.12.1 GA e 9.13.0 GA. È possibile aggiornare queste versioni a patch e release successive di Cloud Volumes ONTAP. Se desideri distribuire versioni successive di Cloud Volumes ONTAP nelle regioni della Cina, contatta l'assistenza NetApp .

Per la disponibilità regionale, fare riferimento a "Mappe delle regioni globali per Cloud Volumes ONTAP" .

05 marzo 2023

Con la versione 3.9.27 del Connector sono state introdotte le seguenti modifiche.

Cloud Volumes ONTAP 9.13.0

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.13.0 in AWS, Azure e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

Supporto 16 TiB e 32 Tib in Azure

Cloud Volumes ONTAP supporta ora dimensioni di disco da 16 TiB e 32 TiB per distribuzioni ad alta disponibilità eseguite su dischi gestiti in Azure.

Scopri di più su "dimensioni dei dischi supportate in Azure" .

licenza MTEKM

La licenza Multi-tenant Encryption Key Management (MTEKM) è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.12.1 GA o successiva.

La gestione delle chiavi esterne multi-tenant consente alle singole VM di archiviazione (SVM) di gestire le proprie chiavi tramite un server KMIP quando si utilizza NetApp Volume Encryption.

"Scopri come crittografare i volumi con le soluzioni di crittografia NetApp" .

Supporto per ambienti senza Internet

Cloud Volumes ONTAP è ora supportato in qualsiasi ambiente cloud che sia completamente isolato da Internet. In questi ambienti è supportata solo la licenza basata sui nodi (BYOL). Le licenze basate sulla capacità non sono supportate. Per iniziare, installa manualmente il software Connector, accedi alla console BlueXP in esecuzione sul Connector, aggiungi la tua licenza BYOL al BlueXP digital wallet e quindi distribuisci Cloud Volumes ONTAP.

- "Installare il connettore in una posizione senza accesso a Internet"
- "Accedi alla console BlueXP sul connettore"
- "Aggiungi una licenza non assegnata"

Flash Cache e alta velocità di scrittura in Google Cloud

Il supporto per Flash Cache, elevata velocità di scrittura e un'unità di trasmissione massima (MTU) elevata di 8.896 byte è ora disponibile per istanze selezionate con la versione Cloud Volumes ONTAP 9.13.0.

Scopri di più su "configurazioni supportate per licenza per Google Cloud" .

05 febbraio 2023

Con la versione 3.9.26 del Connector sono state introdotte le seguenti modifiche.

Creazione di gruppi di posizionamento in AWS

È ora disponibile una nuova impostazione di configurazione per la creazione di gruppi di posizionamento con distribuzioni AWS HA a zona di disponibilità singola (AZ). Ora puoi scegliere di ignorare le creazioni di gruppi di posizionamento non riuscite e consentire il completamento corretto delle distribuzioni AWS HA su una singola zona di disponibilità.

Per informazioni dettagliate su come configurare l'impostazione di creazione del gruppo di posizionamento, fare riferimento a "Configurare la creazione del gruppo di posizionamento per AWS HA Single AZ" .

Aggiornamento della configurazione della zona DNS privata

È ora disponibile una nuova impostazione di configurazione che consente di evitare di creare un collegamento tra una zona DNS privata e una rete virtuale quando si utilizzano i collegamenti privati di Azure. La creazione è abilitata per impostazione predefinita.

"Fornisci a BlueXP i dettagli sul tuo DNS privato di Azure"

Archiviazione WORM e livelli di dati

Ora puoi abilitare contemporaneamente sia il tiering dei dati sia l'archiviazione WORM quando crei un sistema Cloud Volumes ONTAP 9.8 o versione successiva. Abilitando la suddivisione in livelli dei dati con l'archiviazione WORM è possibile suddividere i dati in livelli in un archivio oggetti nel cloud.

"Scopri di più sullo storage WORM."

1 gennaio 2023

Con la versione 3.9.25 del Connector sono state introdotte le seguenti modifiche.

Pacchetti di licenze disponibili in Google Cloud

I pacchetti di licenze basati sulla capacità di Edge Cache e Optimized sono disponibili per Cloud Volumes ONTAP nel Google Cloud Marketplace come offerta con pagamento a consumo o come contratto annuale.

Fare riferimento a "Licenza Cloud Volumes ONTAP" .

Configurazione predefinita per Cloud Volumes ONTAP

La licenza Multi-tenant Encryption Key Management (MTEKM) non è più inclusa nelle nuove distribuzioni Cloud Volumes ONTAP .

Per ulteriori informazioni sulle licenze delle funzionalità ONTAP installate automaticamente con Cloud Volumes ONTAP, fare riferimento a "Configurazione predefinita per Cloud Volumes ONTAP" .

15 dicembre 2022

Cloud Volumes ONTAP 9.12.0

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.12.0 su AWS e Google Cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

08 dicembre 2022

Cloud Volumes ONTAP 9.12.1

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.12.1, che include il supporto per nuove funzionalità e regioni aggiuntive di provider cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP"

04 dicembre 2022

Con la versione 3.9.24 del Connector sono state introdotte le seguenti modifiche.

WORM + Cloud Backup ora disponibile durante la creazione Cloud Volumes ONTAP

La possibilità di attivare le funzionalità WORM (Write Once, Read Many) e Cloud Backup è ora disponibile durante il processo di creazione Cloud Volumes ONTAP .

La regione di Israele ora è supportata in Google Cloud

La regione Israele è ora supportata in Google Cloud per Cloud Volumes ONTAP e Connector per Cloud Volumes ONTAP 9.11.1 P3 e versioni successive.

15 novembre 2022

Con la versione 3.9.23 del Connector sono state introdotte le seguenti modifiche.

Licenza ONTAP S3 in Google Cloud

Una licenza ONTAP S3 è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.12.1 o successiva in Google Cloud Platform.

"Documentazione ONTAP : scopri come configurare e gestire i servizi di archiviazione di oggetti S3"

06 novembre 2022

Con la versione 3.9.23 del Connector sono state introdotte le seguenti modifiche.

Spostamento di gruppi di risorse in Azure

Ora puoi spostare un ambiente di lavoro da un gruppo di risorse a un gruppo di risorse diverso in Azure all'interno della stessa sottoscrizione di Azure.

Per ulteriori informazioni, consulta "Spostamento di gruppi di risorse" .

Certificazione NDMP-copia

NDMP-copy è ora certificato per l'uso con Cloud Volume ONTAP.

Per informazioni su come configurare e utilizzare NDMP, fare riferimento a "Documentazione ONTAP : panoramica della configurazione NDMP" .

Supporto per la crittografia dei dischi gestiti per Azure

È stata aggiunta una nuova autorizzazione di Azure che ora consente di crittografare tutti i dischi gestiti al momento della creazione.

Per maggiori informazioni su questa nuova funzionalità, fare riferimento a "Configurare Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in Azure" .

18 settembre 2022

Con la versione 3.9.22 del Connector sono state introdotte le seguenti modifiche.

Miglioramenti del portafoglio digitale

- Il Portafoglio digitale ora mostra un riepilogo del pacchetto di licenze I/O ottimizzato e della capacità WORM fornita per i sistemi Cloud Volumes ONTAP nel tuo account.

  Questi dettagli possono aiutarti a capire meglio come ti vengono addebitati i costi e se devi acquistare capacità aggiuntiva.

"Scopri come visualizzare la capacità consumata nel tuo account" .

- Ora puoi passare da un metodo di ricarica al metodo di ricarica ottimizzato.

  "Scopri come cambiare i metodi di ricarica" .

Ottimizzare costi e prestazioni

Ora puoi ottimizzare i costi e le prestazioni di un sistema Cloud Volumes ONTAP direttamente da Canvas.

Dopo aver selezionato un ambiente di lavoro, puoi scegliere l'opzione **Ottimizza costi e prestazioni** per modificare il tipo di istanza per Cloud Volumes ONTAP. Scegliere un'istanza di dimensioni più piccole può aiutarti a ridurre i costi, mentre passare a un'istanza di dimensioni maggiori può aiutarti a ottimizzare le prestazioni.

[Uno screenshot dell'opzione Ottimizza costi e prestazioni disponibile nel Canvas dopo aver selezionato un sistema Cloud Volumes ONTAP .]

Notifiche di AutoSupport

BlueXP genererà ora una notifica se un sistema Cloud Volumes ONTAP non è in grado di inviare messaggi AutoSupport . La notifica include un collegamento alle istruzioni che puoi utilizzare per risolvere i problemi di rete.

31 luglio 2022

Con la versione 3.9.21 del Connector sono state introdotte le seguenti modifiche.

licenza MTEKM

La licenza Multi-tenant Encryption Key Management (MTEKM) è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.11.1 o successiva.

La gestione delle chiavi esterne multi-tenant consente alle singole VM di archiviazione (SVM) di gestire le proprie chiavi tramite un server KMIP quando si utilizza NetApp Volume Encryption.

"Scopri come crittografare i volumi con le soluzioni di crittografia NetApp" .

Server proxy

BlueXP ora configura automaticamente i sistemi Cloud Volumes ONTAP per utilizzare il connettore come server proxy, se non è disponibile una connessione Internet in uscita per inviare messaggi AutoSupport .

AutoSupport monitora in modo proattivo lo stato di salute del tuo sistema e invia messaggi al supporto tecnico NetApp .

L'unico requisito è garantire che il gruppo di sicurezza del connettore consenta connessioni *in entrata* sulla porta 3128. Dopo aver distribuito il connettore, sarà necessario aprire questa porta.

Cambia metodo di addebito

Ora è possibile modificare il metodo di addebito per un sistema Cloud Volumes ONTAP che utilizza licenze basate sulla capacità. Ad esempio, se hai distribuito un sistema Cloud Volumes ONTAP con il pacchetto Essentials, puoi modificarlo con il pacchetto Professional se le tue esigenze aziendali cambiano. Questa

funzionalità è disponibile nel Portafoglio digitale.

"Scopri come cambiare i metodi di ricarica" .

Miglioramento del gruppo di sicurezza

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP , l'interfaccia utente consente ora di scegliere se si desidera che il gruppo di sicurezza predefinito consenta il traffico solo all'interno della rete selezionata (opzione consigliata) o di tutte le reti.

[Uno screenshot che mostra l'opzione Consenti traffico all'interno, disponibile nella procedura guidata dell'ambiente di lavoro quando si seleziona un gruppo di sicurezza.]

18 luglio 2022

Nuovi pacchetti di licenze in Azure

Sono disponibili due nuovi pacchetti di licenze basati sulla capacità per Cloud Volumes ONTAP in Azure quando si paga tramite un abbonamento ad Azure Marketplace:

- **Ottimizzato**: paga separatamente la capacità fornita e le operazioni di I/O
- **Edge Cache**: Licenza per "Cache Edge di Cloud Volumes"

"Scopri di più su questi pacchetti di licenza" .

3 luglio 2022

Con la versione 3.9.20 del Connector sono state introdotte le seguenti modifiche.

Portafoglio digitale

Il Portafoglio digitale ora mostra la capacità totale consumata nel tuo account e la capacità consumata per pacchetto di licenza. Questo può aiutarti a capire come ti vengono addebitati i costi e se devi acquistare capacità aggiuntiva.

[Uno screenshot che mostra la pagina del Portafoglio digitale per le licenze basate sulla capacità. La pagina fornisce una panoramica della capacità consumata nel tuo account e poi suddivide la capacità consumata in base al pacchetto di licenza.]

Miglioramento dei volumi elastici

BlueXP ora supporta la funzionalità Amazon EBS Elastic Volumes durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP dall'interfaccia utente. La funzionalità Elastic Volumes è abilitata per impostazione predefinita quando si utilizzano dischi gp3 o io1. È possibile scegliere la capacità iniziale in base alle proprie esigenze di archiviazione e modificarla dopo l'implementazione Cloud Volumes ONTAP .

"Scopri di più sul supporto per Elastic Volumes in AWS" .

Licenza ONTAP S3 in AWS

Una licenza ONTAP S3 è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.11.0 o successiva in AWS.

"Documentazione ONTAP : scopri come configurare e gestire i servizi di archiviazione di oggetti S3"

Nuovo supporto per la regione Azure Cloud

A partire dalla versione 9.10.1, Cloud Volumes ONTAP è ora supportato nella regione Azure West US 3.

"Visualizza l'elenco completo delle regioni supportate per Cloud Volumes ONTAP"

Licenza ONTAP S3 in Azure

Una licenza ONTAP S3 è ora inclusa nei sistemi Cloud Volumes ONTAP nuovi ed esistenti che eseguono la versione 9.9.1 o successiva in Azure.

"Documentazione ONTAP : scopri come configurare e gestire i servizi di archiviazione di oggetti S3"

07 giugno 2022

Con la versione 3.9.19 del Connector sono state introdotte le seguenti modifiche.

Cloud Volumes ONTAP 9.11.1

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.11.1, che include il supporto per nuove funzionalità e regioni aggiuntive di provider cloud.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP"

Nuova vista avanzata

Se è necessario eseguire una gestione avanzata di Cloud Volumes ONTAP, è possibile farlo utilizzando ONTAP System Manager, un'interfaccia di gestione fornita con un sistema ONTAP . Abbiamo incluso l'interfaccia System Manager direttamente in BlueXP , così non dovrai uscire da BlueXP per una gestione avanzata.

Questa visualizzazione avanzata è disponibile come anteprima con Cloud Volumes ONTAP 9.10.0 e versioni successive. Abbiamo intenzione di perfezionare questa esperienza e aggiungere miglioramenti nelle prossime versioni. Inviaci il tuo feedback tramite la chat interna al prodotto.

"Scopri di più sulla Vista avanzata" .

Supporto per Amazon EBS Elastic Volumes

Il supporto per la funzionalità Amazon EBS Elastic Volumes con un aggregato Cloud Volumes ONTAP garantisce prestazioni migliori e capacità aggiuntiva, consentendo al contempo a BlueXP di aumentare automaticamente la capacità del disco sottostante in base alle necessità.

Il supporto per Elastic Volumes è disponibile a partire dai *nuovi* sistemi Cloud Volumes ONTAP 9.11.0 e con i tipi di disco EBS gp3 e io1.

"Scopri di più sul supporto per Elastic Volumes" .

Si noti che il supporto per Elastic Volumes richiede nuove autorizzazioni AWS per il connettore:

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

Assicurati di fornire queste autorizzazioni a ciascun set di credenziali AWS che hai aggiunto a BlueXP. "Visualizza l'ultima policy del connettore per AWS" .

Supporto per la distribuzione di coppie HA in subnet AWS condivise

Cloud Volumes ONTAP 9.11.1 include il supporto per la condivisione AWS VPC. Questa versione del connettore consente di distribuire una coppia HA in una subnet condivisa AWS quando si utilizza l'API.

"Scopri come distribuire una coppia HA in una subnet condivisa" .

Accesso alla rete limitato quando si utilizzano endpoint di servizio

BlueXP ora limita l'accesso alla rete quando si utilizza un endpoint del servizio VNet per le connessioni tra Cloud Volumes ONTAP e gli account di archiviazione. BlueXP utilizza un endpoint di servizio se si disabilitano le connessioni Azure Private Link.

"Scopri di più sulle connessioni Azure Private Link con Cloud Volumes ONTAP" .

Supporto per la creazione di VM di archiviazione in Google Cloud

A partire dalla versione 9.11.1, Cloud Volumes ONTAP in Google Cloud supporta ora più VM di archiviazione. A partire da questa versione del connettore, BlueXP consente di creare VM di archiviazione su coppie Cloud Volumes ONTAP HA in Google Cloud utilizzando l'API.

Il supporto per la creazione di VM di archiviazione richiede nuove autorizzazioni Google Cloud per il connettore:

```
- compute.instanceGroups.get
- compute.addresses.get
```

Si noti che è necessario utilizzare la CLI di ONTAP o System Manager per creare una storage VM su un sistema a nodo singolo.

- "Scopri di più sui limiti di archiviazione delle VM in Google Cloud"
- "Scopri come creare VM di archiviazione per il data serving per Cloud Volumes ONTAP in Google Cloud"

02 maggio 2022

Con la versione 3.9.18 del Connector sono state introdotte le seguenti modifiche.

Cloud Volumes ONTAP 9.11.0

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.11.0.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

Miglioramento degli aggiornamenti del mediatore

Quando BlueXP aggiorna il mediatore per una coppia HA, ora convalida la disponibilità di una nuova immagine del mediatore prima di eliminare il disco di avvio. Questa modifica garantisce che il mediatore possa continuare a funzionare correttamente anche se il processo di aggiornamento non riesce.

La scheda K8s è stata rimossa

La scheda K8s era obsoleta in una versione precedente e ora è stata rimossa.

Contratto annuale in Azure

I pacchetti Essentials e Professional sono ora disponibili in Azure tramite un contratto annuale. Puoi contattare il tuo rappresentante commerciale NetApp per acquistare un contratto annuale. Il contratto è disponibile come offerta privata su Azure Marketplace.

Dopo che NetApp avrà condiviso con te l'offerta privata, potrai selezionare il piano annuale quando ti iscrivi da Azure Marketplace durante la creazione dell'ambiente di lavoro.

"Scopri di più sulle licenze" .

Recupero istantaneo del ghiacciaio S3

Ora puoi archiviare dati a livelli nella classe di archiviazione Glacier Instant Retrieval di Amazon Simple Storage Service (Amazon S3).

"Scopri come modificare la classe di archiviazione per i dati a livelli" .

Nuove autorizzazioni AWS richieste per il connettore

Per creare un gruppo di posizionamento distribuito AWS quando si distribuisce una coppia HA in una singola zona di disponibilità (AZ) sono ora necessarie le seguenti autorizzazioni:

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

Queste autorizzazioni sono ora necessarie per ottimizzare il modo in cui BlueXP crea il gruppo di posizionamento.

Assicurati di fornire queste autorizzazioni a ciascun set di credenziali AWS che hai aggiunto a BlueXP. "Visualizza l'ultima policy del connettore per AWS" .

Nuovo supporto per le regioni di Google Cloud

Cloud Volumes ONTAP è ora supportato nelle seguenti regioni di Google Cloud a partire dalla versione 9.10.1:

- Delhi (asia-sud2)
- Melbourne (Australia-sud-est2)
- Milano (europe-west8) - solo nodo singolo
- Santiago (southamerica-west1) - solo nodo singolo

"Visualizza l'elenco completo delle regioni supportate per Cloud Volumes ONTAP"

Supporto per n2-standard-16 in Google Cloud

Il tipo di macchina n2-standard-16 è ora supportato con Cloud Volumes ONTAP in Google Cloud, a partire dalla versione 9.10.1.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in Google Cloud"

Miglioramenti ai criteri del firewall di Google Cloud

- Quando si crea una coppia Cloud Volumes ONTAP HA in Google Cloud, BlueXP visualizzerà ora tutti i criteri firewall esistenti in una VPC.

  In precedenza, BlueXP non visualizzava alcuna policy in VPC-1, VPC-2 o VPC-3 che non avesse un tag di destinazione.

- Quando crei un sistema Cloud Volumes ONTAP a nodo singolo in Google Cloud, ora puoi scegliere se desideri che il criterio firewall predefinito consenta il traffico solo all'interno della VPC selezionata (consigliato) o di tutte le VPC.

Miglioramento degli account di servizio Google Cloud

Quando selezioni l'account del servizio Google Cloud da utilizzare con Cloud Volumes ONTAP, BlueXP ora visualizza l'indirizzo email associato a ciascun account del servizio. Visualizzare l'indirizzo email può semplificare la distinzione tra account di servizio che condividono lo stesso nome.

[Uno screenshot del campo dell'account di servizio]

3 aprile 2022

Il collegamento al Gestore di sistema è stato rimosso

Abbiamo rimosso il collegamento System Manager che era precedentemente disponibile all'interno di un ambiente di lavoro Cloud Volumes ONTAP .

È comunque possibile connettersi a System Manager immettendo l'indirizzo IP di gestione del cluster in un browser Web connesso al sistema Cloud Volumes ONTAP . "Scopri di più sulla connessione a System Manager" .

Addebito per l'archiviazione WORM

Ora che la tariffa speciale introduttiva è scaduta, ti verrà addebitato un costo per l'utilizzo dello spazio di archiviazione WORM. La tariffazione è oraria, in base alla capacità totale fornita dei volumi WORM. Ciò vale per i sistemi Cloud Volumes ONTAP nuovi ed esistenti.

"Scopri i prezzi per l'archiviazione WORM" .

27 febbraio 2022

Con la versione 3.9.16 del Connector sono state introdotte le seguenti modifiche.

Procedura guidata del volume riprogettata

La procedura guidata per la creazione di un nuovo volume introdotta di recente è ora disponibile quando si crea un volume su un aggregato specifico tramite l'opzione **Allocazione avanzata**.

"Scopri come creare volumi su un aggregato specifico" .

09 febbraio 2022

Aggiornamenti del Marketplace

- I pacchetti Essentials e Professional sono ora disponibili in tutti i marketplace dei provider cloud.

  Questi metodi di addebito in base alla capacità consentono di pagare a ore o di acquistare un contratto annuale direttamente dal proprio fornitore di servizi cloud. Hai ancora la possibilità di acquistare una licenza in base alla capacità direttamente da NetApp.

  Se hai già un abbonamento in un marketplace cloud, verrai automaticamente abbonato anche a queste nuove offerte. Quando si distribuisce un nuovo ambiente di lavoro Cloud Volumes ONTAP , è possibile scegliere la tariffazione in base alla capacità.

  Se sei un nuovo cliente, BlueXP ti chiederà di iscriverti quando crei un nuovo ambiente di lavoro.

- La concessione di licenze per nodo da tutti i marketplace dei provider cloud è obsoleta e non è più disponibile per i nuovi abbonati. Sono inclusi i contratti annuali e gli abbonamenti orari (Explore, Standard e Premium).

  Questo metodo di addebito è ancora disponibile per i clienti esistenti che hanno un abbonamento attivo.

"Scopri di più sulle opzioni di licenza per Cloud Volumes ONTAP" .

06 febbraio 2022

Scambia licenze non assegnate

Se disponi di una licenza basata su nodi non assegnata per Cloud Volumes ONTAP che non hai utilizzato, ora puoi scambiare la licenza convertendola in una licenza Cloud Backup, una licenza Cloud Data Sense o una licenza Cloud Tiering.

Questa azione revoca la licenza Cloud Volumes ONTAP e crea una licenza equivalente in dollari per il servizio con la stessa data di scadenza.

"Scopri come scambiare licenze basate su nodi non assegnati" .

30 gennaio 2022

Con la versione 3.9.15 del Connector sono state introdotte le seguenti modifiche.

Selezione delle licenze riprogettata

Abbiamo riprogettato la schermata di selezione delle licenze durante la creazione di un nuovo ambiente di lavoro Cloud Volumes ONTAP . Le modifiche evidenziano i metodi di addebito in base alla capacità introdotti a luglio 2021 e supportano le prossime offerte tramite i marketplace dei provider cloud.

Aggiornamento del portafoglio digitale

Abbiamo aggiornato il **Portafoglio digitale** consolidando le licenze Cloud Volumes ONTAP in un'unica scheda.

02 gennaio 2022

Con la versione 3.9.14 del Connector sono state introdotte le seguenti modifiche.

Supporto per tipi aggiuntivi di VM di Azure

Cloud Volumes ONTAP è ora supportato con i seguenti tipi di VM in Microsoft Azure, a partire dalla versione 9.10.1:

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

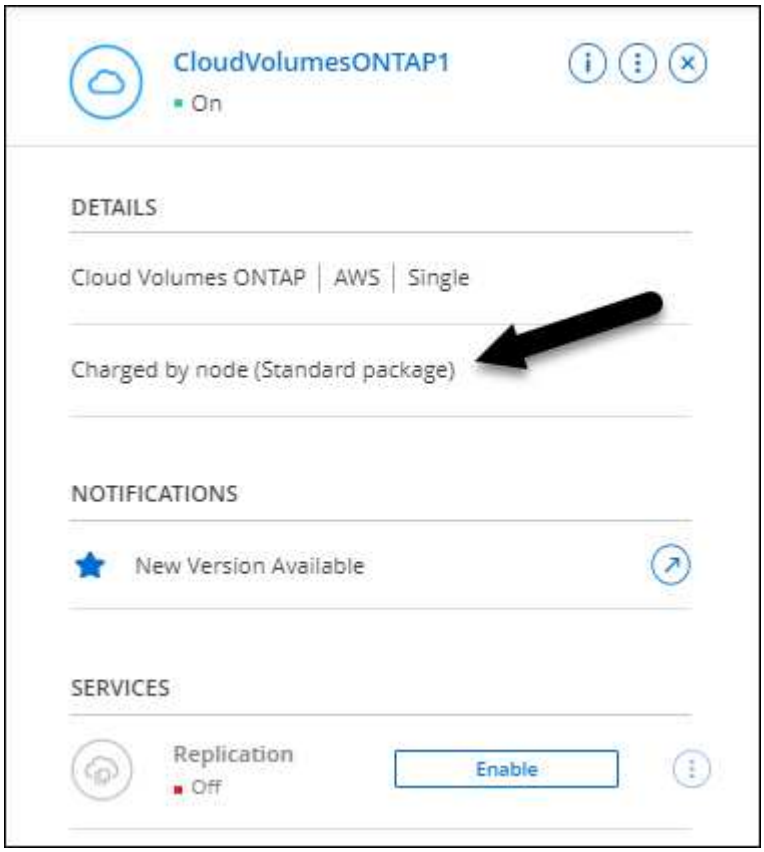
Vai al "Note sulla versione Cloud Volumes ONTAP" per maggiori dettagli sulle configurazioni supportate.

Aggiornamento della ricarica FlexClone

Se usi un "licenza basata sulla capacità" per Cloud Volumes ONTAP, non ti verrà più addebitata la capacità utilizzata dai volumi FlexClone .

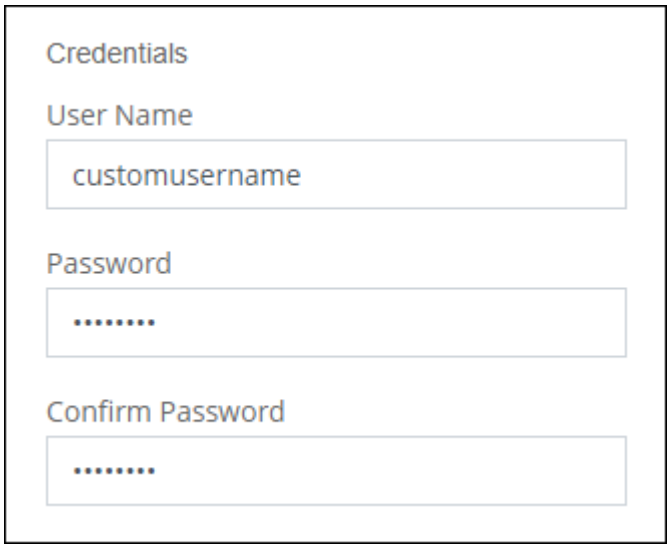
Ora viene visualizzato il metodo di ricarica

BlueXP ora mostra il metodo di addebito per ciascun ambiente di lavoro Cloud Volumes ONTAP nel pannello destro di Canvas.



Scegli il tuo nome utente

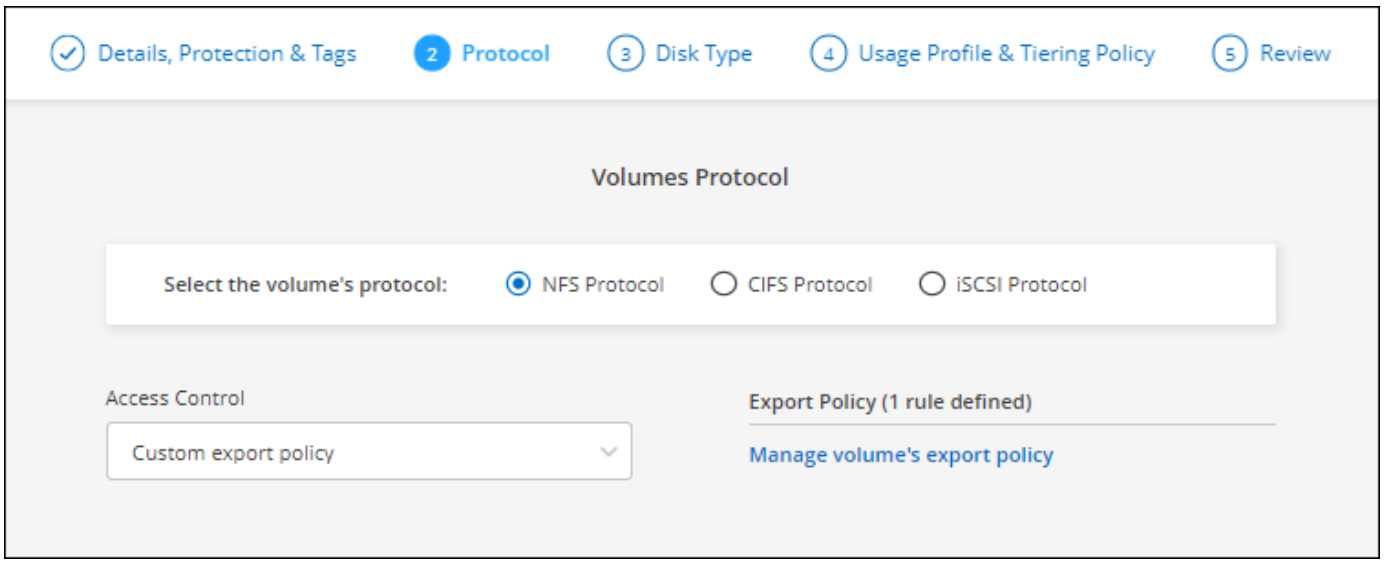
Quando si crea un ambiente di lavoro Cloud Volumes ONTAP , ora è possibile immettere il nome utente preferito, anziché il nome utente amministratore predefinito.



Miglioramenti nella creazione del volume

Abbiamo apportato alcuni miglioramenti alla creazione dei volumi:

- Abbiamo riprogettato la procedura guidata di creazione del volume per semplificarne l'utilizzo.
- Ora puoi scegliere una policy di esportazione personalizzata per NFS.



28 novembre 2021

Con la versione 3.9.13 del Connector sono state introdotte le seguenti modifiche.

Cloud Volumes ONTAP 9.10.1

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.10.1.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

Abbonamenti NetApp Keystone

Ora puoi utilizzare gli abbonamenti Keystone per pagare le coppie Cloud Volumes ONTAP HA.

Un abbonamento Keystone è un servizio basato su abbonamento con pagamento in base alla crescita che offre un'esperienza cloud ibrida senza interruzioni per coloro che preferiscono modelli di consumo OpEx a CapEx anticipati o leasing.

Un abbonamento Keystone è supportato con tutte le nuove versioni di Cloud Volumes ONTAP che è possibile distribuire da BlueXP.

- "Scopri di più sugli abbonamenti NetApp Keystone" .
- "Scopri come iniziare a utilizzare gli abbonamenti Keystone in BlueXP" .

Nuovo supporto per la regione AWS

Cloud Volumes ONTAP è ora supportato nella regione AWS Asia Pacific (Osaka) (ap-northeast-3).

Riduzione del porto

Le porte 8023 e 49000 non sono più aperte sui sistemi Cloud Volumes ONTAP in Azure, sia per i sistemi a nodo singolo che per le coppie HA.

Questa modifica si applica ai *nuovi* sistemi Cloud Volumes ONTAP a partire dalla versione 3.9.13 del Connector.

04 ottobre 2021

Con la versione 3.9.11 del Connector sono state introdotte le seguenti modifiche.

Cloud Volumes ONTAP 9.10.0

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.10.0.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

Tempo di distribuzione ridotto

Abbiamo ridotto il tempo necessario per distribuire un ambiente di lavoro Cloud Volumes ONTAP in Microsoft Azure o in Google Cloud quando è abilitata la normale velocità di scrittura. Il tempo di implementazione è ora in media più breve di 3-4 minuti.

02 settembre 2021

Con la versione 3.9.10 del Connector sono state introdotte le seguenti modifiche.

Chiave di crittografia gestita dal cliente in Azure

I dati vengono crittografati automaticamente su Cloud Volumes ONTAP in Azure utilizzando "Crittografia del servizio di archiviazione di Azure" con una chiave gestita da Microsoft. Ma ora puoi utilizzare la tua chiave di crittografia gestita dal cliente completando i seguenti passaggi:

1. Da Azure, crea un archivio chiavi e quindi genera una chiave in tale archivio.
2. Da BlueXP, utilizzare l'API per creare un ambiente di lavoro Cloud Volumes ONTAP che utilizzi la chiave.

"Scopri di più su questi passaggi" .

07 luglio 2021

Con la versione 3.9.8 del Connector sono state introdotte le seguenti modifiche.

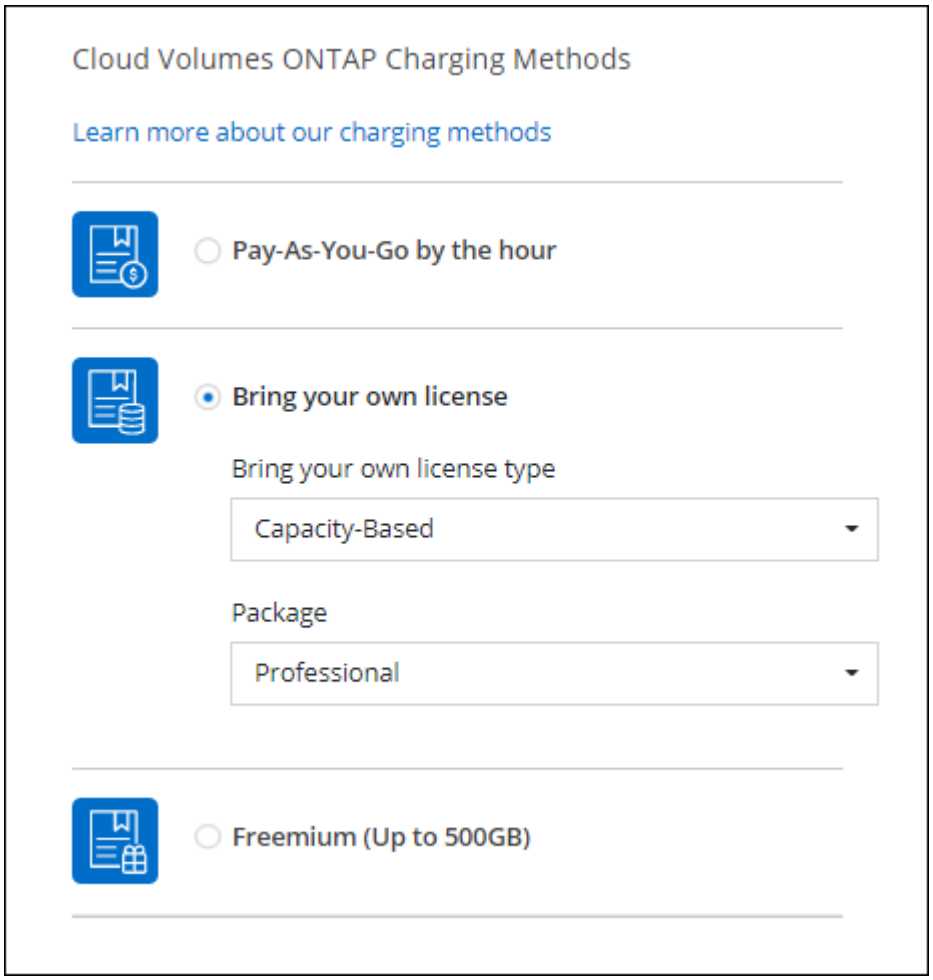
Nuovi metodi di ricarica

Sono disponibili nuovi metodi di addebito per Cloud Volumes ONTAP.

- **BYOL basato sulla capacità**: una licenza basata sulla capacità consente di pagare Cloud Volumes ONTAP per TiB di capacità. La licenza è associata al tuo account NetApp e ti consente di creare più sistemi Cloud Volumes ONTAP , a condizione che la tua licenza disponga di capacità sufficiente. Le licenze basate sulla capacità sono disponibili sotto forma di pacchetto, *Essentials* o *Professional*.
- **Offerta Freemium**: Freemium ti consente di utilizzare gratuitamente tutte le funzionalità Cloud Volumes ONTAP di NetApp (si applicano comunque i costi del provider cloud). La capacità disponibile per sistema è limitata a 500 GiB e non è previsto alcun contratto di supporto. Puoi avere fino a 10 sistemi Freemium.

  "Scopri di più su queste opzioni di licenza" .

  Ecco un esempio dei metodi di addebito tra cui puoi scegliere:



Archiviazione WORM disponibile per uso generale

Lo storage WORM (Write Once, Read Many) non è più disponibile in anteprima ed è ora disponibile per l'uso generale con Cloud Volumes ONTAP. "Scopri di più sullo storage WORM" .

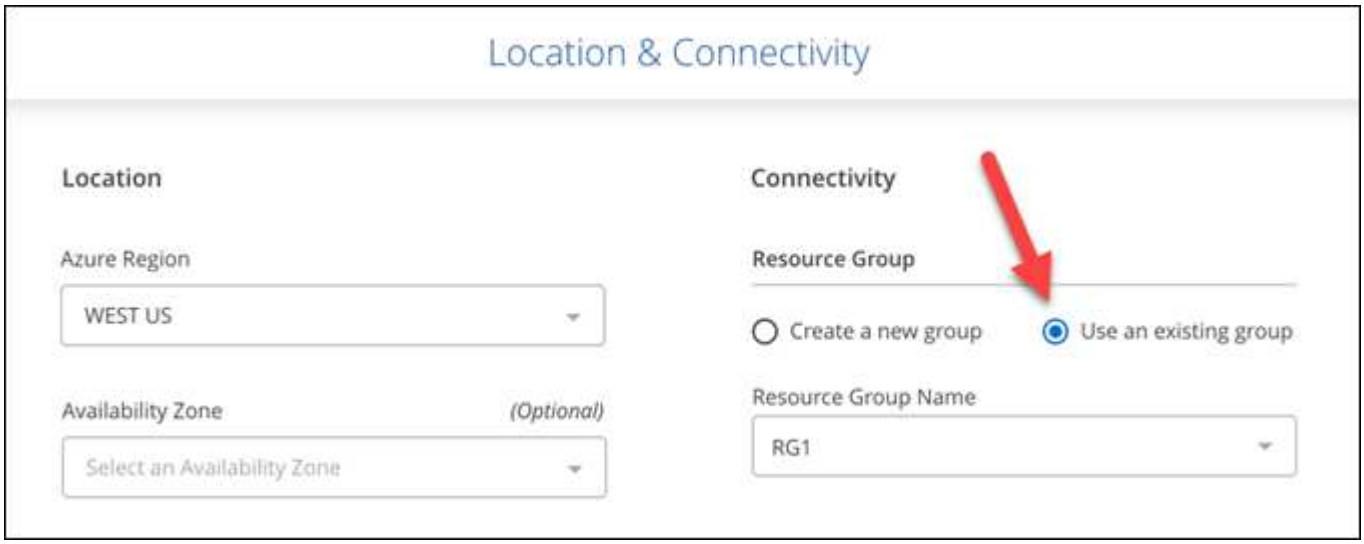
Supporto per m5dn.24xlarge in AWS

A partire dalla versione 9.9.1, Cloud Volumes ONTAP supporta il tipo di istanza m5dn.24xlarge con i seguenti metodi di addebito: PAYGO Premium, Bring Your Own License (BYOL) e Freemium.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in AWS" .

Seleziona gruppi di risorse di Azure esistenti

Quando si crea un sistema Cloud Volumes ONTAP in Azure, ora è possibile selezionare un gruppo di risorse esistente per la macchina virtuale e le risorse associate.



Le seguenti autorizzazioni consentono a BlueXP di rimuovere le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di distribuzione o eliminazione:

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

Assicurati di fornire queste autorizzazioni a ogni set di credenziali di Azure che hai aggiunto a BlueXP. "Visualizza i criteri più recenti del connettore per Azure" .

L'accesso pubblico ai BLOB è ora disabilitato in Azure

Come miglioramento della sicurezza, BlueXP ora disabilita l'**accesso pubblico al Blob** durante la creazione di un account di archiviazione per Cloud Volumes ONTAP.

Miglioramento di Azure Private Link

Per impostazione predefinita, BlueXP ora abilita una connessione Azure Private Link sull'account di archiviazione della diagnostica di avvio per i nuovi sistemi Cloud Volumes ONTAP .

Ciò significa che *tutti* gli account di archiviazione per Cloud Volumes ONTAP utilizzeranno ora un collegamento privato.

"Scopri di più sull'utilizzo di un collegamento privato di Azure con Cloud Volumes ONTAP" .

Dischi persistenti bilanciati in Google Cloud

A partire dalla versione 9.9.1, Cloud Volumes ONTAP supporta ora i dischi persistenti bilanciati (pd-balanced).

Questi SSD bilanciano prestazioni e costi offrendo IOPS inferiori per GiB.

custom-4-16384 non è più supportato in Google Cloud

Il tipo di macchina custom-4-16384 non è più supportato con i nuovi sistemi Cloud Volumes ONTAP .

Se disponi di un sistema esistente in esecuzione su questo tipo di macchina, puoi continuare a utilizzarlo, ma ti consigliamo di passare al tipo di macchina n2-standard-4.

"Visualizza le configurazioni supportate per Cloud Volumes ONTAP in Google Cloud".

30 maggio 2021

Con la versione 3.9.7 del Connector sono state introdotte le seguenti modifiche.

Nuovo pacchetto professionale in AWS

Un nuovo pacchetto professionale consente di raggruppare Cloud Volumes ONTAP e Cloud Backup Service utilizzando un contratto annuale di AWS Marketplace. Il pagamento avviene per TiB. Questo abbonamento non consente di eseguire il backup dei dati in locale.

Se scegli questa opzione di pagamento, puoi fornire fino a 2 PiB per sistema Cloud Volumes ONTAP tramite dischi EBS e suddivisione in livelli nell'archiviazione di oggetti S3 (nodo singolo o HA).

Vai al "Pagina AWS Marketplace" per visualizzare i dettagli dei prezzi e andare al "Note sulla versione Cloud Volumes ONTAP" per saperne di più su questa opzione di licenza.

Tag sui volumi EBS in AWS

BlueXP ora aggiunge tag ai volumi EBS quando crea un nuovo ambiente di lavoro Cloud Volumes ONTAP . I tag sono stati creati in precedenza dopo l'implementazione Cloud Volumes ONTAP .

Questa modifica può essere utile se la tua organizzazione utilizza criteri di controllo dei servizi (SCP) per gestire le autorizzazioni.

Periodo di raffreddamento minimo per la politica di auto-tiering

Se hai abilitato il tiering dei dati su un volume utilizzando il criterio di tiering *auto*, ora puoi regolare il periodo di raffreddamento minimo utilizzando l'API.

"Scopri come regolare il periodo minimo di raffreddamento."

Miglioramento delle policy di esportazione personalizzate

Quando si crea un nuovo volume NFS, BlueXP ora visualizza i criteri di esportazione personalizzati in ordine crescente, semplificando la ricerca del criterio di esportazione desiderato.

Eliminazione dei vecchi snapshot cloud

BlueXP ora elimina gli snapshot cloud più vecchi dei dischi root e boot creati quando viene distribuito un sistema Cloud Volumes ONTAP e ogni volta che viene spento. Vengono conservati solo i due snapshot più recenti sia per il volume root che per quello di avvio.

Questo miglioramento aiuta a ridurre i costi del provider cloud rimuovendo gli snapshot non più necessari.

Si noti che un connettore richiede una nuova autorizzazione per eliminare gli snapshot di Azure. "Visualizza i criteri più recenti del connettore per Azure" .

```
"Microsoft.Compute/snapshots/delete"
```

24 maggio 2021

Cloud Volumes ONTAP 9.9.1

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.9.1.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

11 aprile 2021

Con la versione 3.9.5 del Connector sono state introdotte le seguenti modifiche.

Segnalazione dello spazio logico

BlueXP ora consente la creazione di report sullo spazio logico sulla VM di archiviazione iniziale creata per Cloud Volumes ONTAP.

Quando lo spazio viene segnalato in modo logico, ONTAP segnala lo spazio del volume in modo tale che tutto lo spazio fisico risparmiato dalle funzionalità di efficienza di archiviazione venga segnalato come utilizzato.

Supporto per dischi gp3 in AWS

Cloud Volumes ONTAP supporta ora i dischi *General Purpose SSD (gp3)*, a partire dalla versione 9.7. I dischi gp3 sono gli SSD più economici che bilanciano costi e prestazioni per un'ampia gamma di carichi di lavoro.

"Dimensiona il tuo sistema in AWS" .

I dischi HDD freddi non sono più supportati in AWS

Cloud Volumes ONTAP non supporta più i dischi Cold HDD (sc1).

TLS 1.2 per gli account di archiviazione di Azure

Quando BlueXP crea account di archiviazione in Azure per Cloud Volumes ONTAP, la versione TLS per l'account di archiviazione è ora la versione 1.2.

08 marzo 2021

Con la versione 3.9.4 del Connector sono state introdotte le seguenti modifiche.

Cloud Volumes ONTAP 9.9.0

BlueXP ora può distribuire e gestire Cloud Volumes ONTAP 9.9.0.

"Scopri le nuove funzionalità incluse in questa versione di Cloud Volumes ONTAP" .

Supporto per l'ambiente AWS C2S

Ora puoi distribuire Cloud Volumes ONTAP 9.8 nell'ambiente AWS Commercial Cloud Services (C2S).

"Distribuisci Cloud Volumes ONTAP in AWS Secret Cloud o AWS Top Secret Cloud" .

Crittografia AWS con CMK gestite dal cliente

BlueXP ha sempre consentito di crittografare i dati Cloud Volumes ONTAP utilizzando AWS Key Management Service (KMS). A partire da Cloud Volumes ONTAP 9.9.0, i dati sui dischi EBS e i dati suddivisi in livelli S3 vengono crittografati se si seleziona una CMK gestita dal cliente. In precedenza, venivano crittografati solo i dati EBS.

Tieni presente che dovrai fornire al ruolo IAM di Cloud Volumes ONTAP l'accesso per utilizzare la CMK.

"Scopri di più sulla configurazione di AWS KMS con Cloud Volumes ONTAP" .

Supporto per Azure DoD

Ora puoi distribuire Cloud Volumes ONTAP 9.8 in Azure Department of Defense (DoD) Impact Level 6 (IL6).

Riduzione degli indirizzi IP in Google Cloud

Abbiamo ridotto il numero di indirizzi IP richiesti per Cloud Volumes ONTAP 9.8 e versioni successive in Google Cloud. Per impostazione predefinita, è richiesto un indirizzo IP in meno (abbiamo unificato il LIF intercluster con il LIF di gestione dei nodi). È anche possibile saltare la creazione del LIF di gestione SVM quando si utilizza l'API, il che ridurrebbe la necessità di un indirizzo IP aggiuntivo.

"Scopri di più sui requisiti degli indirizzi IP in Google Cloud" .

Supporto VPC condiviso in Google Cloud

Quando distribuisci una coppia Cloud Volumes ONTAP HA in Google Cloud, ora puoi scegliere VPC condivise per VPC-1, VPC-2 e VPC-3. In precedenza, solo VPC-0 poteva essere una VPC condivisa. Questa modifica è supportata con Cloud Volumes ONTAP 9.8 e versioni successive.

"Scopri di più sui requisiti di rete di Google Cloud" .

04 gennaio 2021

Con la versione 3.9.2 del Connector sono state introdotte le seguenti modifiche.

Avamposti AWS

Qualche mese fa abbiamo annunciato che Cloud Volumes ONTAP aveva ottenuto la designazione Amazon Web Services (AWS) Outposts Ready. Oggi siamo lieti di annunciare che abbiamo convalidato BlueXP e Cloud Volumes ONTAP con AWS Outposts.

Se disponi di un AWS Outpost, puoi distribuire Cloud Volumes ONTAP in quell'Outpost selezionando l'Outpost

VPC nella procedura guidata Ambiente di lavoro. L'esperienza è la stessa di qualsiasi altra VPC residente in AWS. Tieni presente che dovrai prima distribuire un connettore nel tuo AWS Outpost.

Ci sono alcune limitazioni da sottolineare:

- Al momento sono supportati solo i sistemi Cloud Volumes ONTAP a nodo singolo
- Le istanze EC2 che puoi utilizzare con Cloud Volumes ONTAP sono limitate a quelle disponibili nel tuo Outpost
- Al momento sono supportati solo gli SSD General Purpose (gp2)

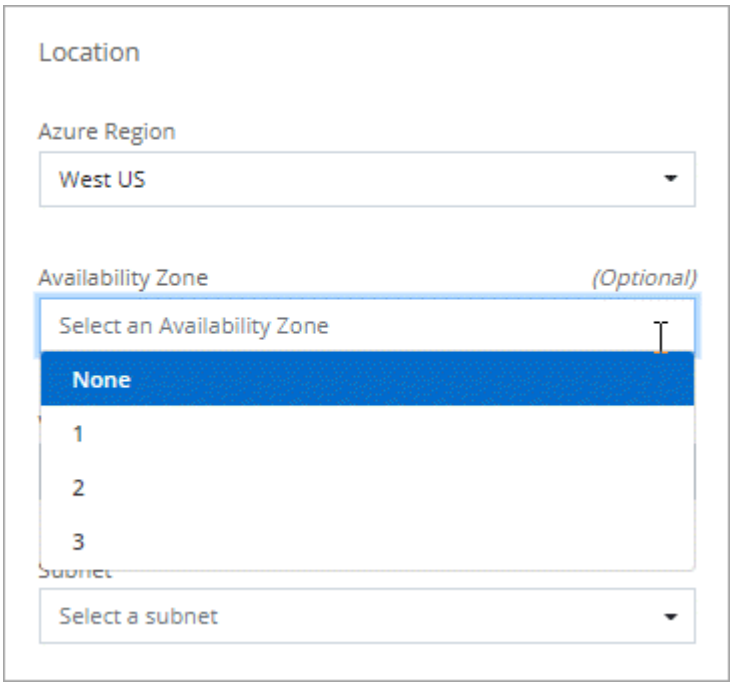
Ultra SSD VNVRAM nelle regioni di Azure supportate

Cloud Volumes ONTAP può ora utilizzare un Ultra SSD come VNVRAM quando si utilizza il tipo di VM E32s_v3 con un sistema a nodo singolo "in qualsiasi regione di Azure supportata".

La VNVRAM garantisce migliori prestazioni di scrittura.

Scegliere una zona di disponibilità in Azure

Ora puoi scegliere la zona di disponibilità in cui desideri distribuire un sistema Cloud Volumes ONTAP a nodo singolo. Se non selezioni una AZ, BlueXP ne selezionerà una per te.



Dischi più grandi in Google Cloud

Cloud Volumes ONTAP ora supporta dischi da 64 TB in Google Cloud.

La capacità massima del sistema con soli dischi rimane a 256 TB a causa dei limiti di Google Cloud.

Nuovi tipi di macchine in Google Cloud

Cloud Volumes ONTAP ora supporta i seguenti tipi di macchine:

- n2-standard-4 con licenza Explore e con BYOL
- n2-standard-8 con licenza Standard e con BYOL
- n2-standard-32 con licenza Premium e con BYOL

03 novembre 2020

Con la versione 3.9.0 del Connector sono state introdotte le seguenti modifiche.

Collegamento privato di Azure per Cloud Volumes ONTAP

Per impostazione predefinita, BlueXP ora abilita una connessione Azure Private Link tra Cloud Volumes ONTAP e i relativi account di archiviazione associati. Un collegamento privato protegge le connessioni tra gli endpoint in Azure.

- "Scopri di più sui collegamenti privati di Azure"
- "Scopri di più sull'utilizzo di un collegamento privato di Azure con Cloud Volumes ONTAP"

Limitazioni note

Le limitazioni note identificano piattaforme, dispositivi o funzioni che non sono supportati da questa versione del prodotto o che non interagiscono correttamente con esso. Esamina attentamente queste limitazioni.

Queste limitazioni sono specifiche della gestione Cloud Volumes ONTAP nella NetApp Console. Per visualizzare le limitazioni del software Cloud Volumes ONTAP stesso, "vai alle Note sulla versione Cloud Volumes ONTAP" .

La console non supporta la creazione di volumi FlexGroup

Sebbene Cloud Volumes ONTAP supporti i volumi FlexGroup , la Console al momento non supporta la creazione di volumi FlexGroup . Se si crea un volume FlexGroup da ONTAP System Manager o da ONTAP CLI, è necessario impostare la modalità di gestione della capacità nella console su `Manual` . `Automatic` la modalità potrebbe non funzionare correttamente con i volumi FlexGroup .

La possibilità di creare volumi FlexGroup nella Console è prevista per una versione futura.

La console non supporta S3 con Cloud Volumes ONTAP

Sebbene Cloud Volumes ONTAP supporti S3 come opzione per lo storage scale-out, la Console non offre alcuna funzionalità di gestione per questa funzionalità. L'utilizzo della CLI è la best practice per configurare l'accesso client S3 da Cloud Volumes ONTAP. Per dettagli, consultare il "Guida alla configurazione ONTAP S3".

"Scopri di più sul supporto di Cloud Volumes ONTAP per ONTAP S3 e altri protocolli client".

La console non supporta il ripristino di emergenza per le VM di archiviazione

La console non fornisce alcun supporto di configurazione o orchestrazione per il ripristino di emergenza delle VM di archiviazione (SVM). È necessario utilizzare ONTAP System Manager o ONTAP CLI.

"Scopri di più sul disaster recovery SVM" .

Note sulla versione Cloud Volumes ONTAP

Le note di rilascio per Cloud Volumes ONTAP forniscono informazioni specifiche sulla versione. Novità della versione, configurazioni supportate, limiti di archiviazione e qualsiasi limitazione o problema noto che potrebbe influire sulla funzionalità del prodotto.

"Vai alle note sulla versione Cloud Volumes ONTAP"

Iniziare

Scopri di più su Cloud Volumes ONTAP

Cloud Volumes ONTAP ti consente di ottimizzare i costi e le prestazioni dello storage cloud, migliorando al contempo la protezione, la sicurezza e la conformità dei dati.

Cloud Volumes ONTAP è un dispositivo di archiviazione esclusivamente software che esegue il software di gestione dati ONTAP nel cloud. Fornisce storage di livello aziendale con le seguenti caratteristiche principali:

- Efficienza di archiviazione

  Sfrutta la deduplicazione dei dati integrata, la compressione dei dati, il thin provisioning e la clonazione per ridurre al minimo i costi di archiviazione.

- Alta disponibilità

  Garantisci l'affidabilità aziendale e la continuità operativa in caso di guasti nel tuo ambiente cloud.

- Protezione dei dati

  Cloud Volumes ONTAP sfrutta SnapMirror, la tecnologia di replicazione leader del settore di NetApp, per replicare i dati on-premise sul cloud, in modo da avere facilmente copie secondarie disponibili per più casi d'uso.

  Cloud Volumes ONTAP si integra anche con NetApp Backup and Recovery per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati cloud.

  "Scopri di più su Backup e Ripristino"

- Livelli dei dati

  Passa da pool di archiviazione ad alte e basse prestazioni su richiesta senza dover disconnettere le applicazioni.

- Coerenza dell'applicazione

  Garantire la coerenza delle copie di NetApp Snapshot utilizzando NetApp SnapCenter.

  "Scopri di più su SnapCenter"

- Sicurezza dei dati

  Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.

- Controlli di conformità alla privacy

  L'integrazione con NetApp Data Classification ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

  "Scopri di più sulla classificazione dei dati"

Le licenze per le funzionalità ONTAP sono incluse in Cloud Volumes ONTAP.

"Visualizza le configurazioni Cloud Volumes ONTAP supportate"

"Scopri di più su Cloud Volumes ONTAP"

Versioni ONTAP supportate per le distribuzioni Cloud Volumes ONTAP

La NetApp Console consente di scegliere tra diverse versioni ONTAP quando si aggiunge un sistema Cloud Volumes ONTAP .

Le versioni di Cloud Volumes ONTAP diverse da quelle elencate qui non sono disponibili per nuove distribuzioni. La patch o la versione generica (General Availability) in una release qui rappresenta la versione base disponibile per la distribuzione. Per dettagli sulle patch disponibili, fare riferimento alle "note di rilascio versionate" per ciascuna release.

Per informazioni sull'upgrade, fare riferimento a "Percorsi di aggiornamento supportati".

AWS

Nodo singolo

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5
- 9.5 P6

coppia HA

- 9.18.1
- 9.17.1 P1
- 9.16.1

- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5
- 9.5 P6

Azzurro

Nodo singolo

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

coppia HA

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

Nodo singolo

- 9.18.1

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5

coppia HA

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8

Inizia ad usare Amazon Web Services

Avvio rapido per Cloud Volumes ONTAP in AWS

Inizia a usare Cloud Volumes ONTAP in AWS in pochi passaggi.

1 Creare un agente Console

Se non hai un "Agente console" eppure devi crearne uno. "Scopri come creare un agente Console in AWS" .

Tieni presente che se vuoi distribuire Cloud Volumes ONTAP in una subnet in cui non è disponibile l'accesso a Internet, devi installare manualmente l'agente Console e accedere all'interfaccia utente NetApp Console in esecuzione su tale agente Console. "Scopri come installare manualmente l'agente Console in una posizione senza accesso a Internet" .

2 Pianifica la tua configurazione

La Console offre pacchetti preconfigurati che soddisfano i requisiti del tuo carico di lavoro, oppure puoi creare la tua configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione. "Saperne di più" .

3 Configura la tua rete

1. Assicurati che la tua VPC e le tue subnet supportino la connettività tra l'agente della console e Cloud Volumes ONTAP.
2. Abilita l'accesso a Internet in uscita dalla VPC di destinazione per NetApp AutoSupport.

   Questo passaggio non è necessario se si distribuisce Cloud Volumes ONTAP in una posizione in cui non è disponibile l'accesso a Internet.

3. Configura un endpoint VPC per il servizio Amazon Simple Storage Service (Amazon S3).

   È necessario un endpoint VPC se si desidera suddividere i dati inattivi da Cloud Volumes ONTAP in un archivio di oggetti a basso costo.

"Scopri di più sui requisiti di rete" .

4 Configurare AWS KMS

Se si desidera utilizzare la crittografia Amazon con Cloud Volumes ONTAP, è necessario assicurarsi che esista una Customer Master Key (CMK) attiva. È inoltre necessario modificare la policy delle chiavi per ogni CMK aggiungendo il ruolo IAM che fornisce le autorizzazioni all'agente della console come *utente chiave*. "Saperne di più" .

5 Avvia Cloud Volumes ONTAP tramite la console

Fare clic su **Aggiungi sistema**, selezionare il tipo di sistema che si desidera distribuire e completare i passaggi della procedura guidata. "Leggi le istruzioni passo passo" .

Link correlati

- "Creare un agente console per AWS"

- "Creare un agente della console da AWS Marketplace"
- "Installa e configura un agente Console in locale"
- "Autorizzazioni AWS per l'agente della console"

Pianifica la configurazione Cloud Volumes ONTAP in AWS

Quando distribuisci Cloud Volumes ONTAP in AWS, puoi scegliere un sistema preconfigurato che soddisfi i requisiti del tuo carico di lavoro oppure puoi creare una configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione.

Scegli una licenza Cloud Volumes ONTAP

Sono disponibili diverse opzioni di licenza per Cloud Volumes ONTAP. Ogni opzione ti consente di scegliere il modello di consumo più adatto alle tue esigenze.

- "Scopri le opzioni di licenza per Cloud Volumes ONTAP"
- "Scopri come impostare le licenze"

Scegli una regione supportata

Cloud Volumes ONTAP è supportato nella maggior parte delle regioni AWS. "Visualizza l'elenco completo delle regioni supportate" .

Per poter creare e gestire risorse in tali regioni, è necessario abilitare le regioni AWS più recenti. "Documentazione AWS: scopri come abilitare una regione" .

Scegli una zona locale supportata

La selezione di una zona locale è facoltativa. Cloud Volumes ONTAP è supportato in alcune zone locali AWS, tra cui Singapore. Cloud Volumes ONTAP in AWS supporta solo la modalità ad alta disponibilità (HA) in una singola zona di disponibilità. Le distribuzioni a nodo singolo non sono supportate.

> Cloud Volumes ONTAP non supporta il tiering dei dati e il tiering del cloud nelle zone locali AWS. Inoltre, le zone locali con istanze che non sono state qualificate per Cloud Volumes ONTAP non sono supportate. Un esempio è Miami, che non è disponibile come zona locale perché ha solo istanze Gen6 non supportate e non qualificate.

"Documentazione AWS: visualizza l'elenco completo delle zone locali" . Le zone locali devono essere abilitate prima di poter creare e gestire risorse in tali zone.

"Documentazione AWS: Introduzione alle zone locali AWS" .

Scegli un'istanza supportata

Cloud Volumes ONTAP supporta diversi tipi di istanza, a seconda del tipo di licenza scelto.

"Configurazioni supportate per Cloud Volumes ONTAP in AWS"

Comprendere i limiti di archiviazione

Il limite di capacità raw per un sistema Cloud Volumes ONTAP è legato alla licenza. Ulteriori limiti incidono sulle dimensioni degli aggregati e sui volumi. Quando pianifichi la tua configurazione, dovresti essere consapevole di questi limiti.

"Limiti di archiviazione per Cloud Volumes ONTAP in AWS"

Dimensiona il tuo sistema in AWS

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di prestazioni e capacità. Quando si sceglie un tipo di istanza, un tipo di disco e una dimensione del disco, è necessario tenere presenti alcuni punti chiave:

Tipo di istanza

- Adatta i requisiti del carico di lavoro alla velocità effettiva e agli IOPS massimi per ogni tipo di istanza EC2.
- Se più utenti scrivono contemporaneamente sul sistema, scegliere un tipo di istanza che abbia CPU sufficienti per gestire le richieste.
- Se hai un'applicazione che legge principalmente, scegli un sistema con RAM sufficiente.
  - "Documentazione AWS: Tipi di istanze Amazon EC2"
  - "Documentazione AWS: istanze ottimizzate per Amazon EBS"

Tipo di disco EBS

A livello generale, le differenze tra i tipi di dischi EBS sono le seguenti. Per saperne di più sui casi d'uso dei dischi EBS, fare riferimento a "Documentazione AWS: Tipi di volume EBS" .

- I dischi *General Purpose SSD (gp3)* sono gli SSD più economici che bilanciano costi e prestazioni per un'ampia gamma di carichi di lavoro. Le prestazioni sono definite in termini di IOPS e throughput. I dischi gp3 sono supportati con Cloud Volumes ONTAP 9.7 e versioni successive.

  Quando si seleziona un disco gp3, la NetApp Console inserisce i valori IOPS e di throughput predefiniti che garantiscono prestazioni equivalenti a quelle di un disco gp2 in base alle dimensioni del disco selezionato. È possibile aumentare i valori per ottenere prestazioni migliori a un costo maggiore, ma non supportiamo valori inferiori perché potrebbero comportare prestazioni inferiori. In breve, mantenete i valori predefiniti oppure aumentateli. Non abbassarli. "Documentazione AWS: Scopri di più sui dischi gp3 e sulle loro prestazioni" .

  Si noti che Cloud Volumes ONTAP supporta la funzionalità Amazon EBS Elastic Volumes con dischi gp3. "Scopri di più sul supporto di Elastic Volumes" .

- I dischi *SSD per uso generale (gp2)* bilanciano costi e prestazioni per un'ampia gamma di carichi di lavoro. Le prestazioni sono definite in termini di IOPS.
- I dischi SSD *Provisioned IOPS (io1)* sono destinati ad applicazioni critiche che richiedono le massime prestazioni a un costo più elevato.

  Si noti che Cloud Volumes ONTAP supporta la funzionalità Amazon EBS Elastic Volumes con dischi io1. "Scopri di più sul supporto di Elastic Volumes" .

- I dischi *Throughput Optimized HDD (st1)* sono adatti a carichi di lavoro a cui si accede frequentemente e che richiedono un throughput rapido e costante a un prezzo inferiore.

Il tiering dei dati su Amazon Simple Storage Service (Amazon S3) non è supportato se il tuo sistema Cloud Volumes ONTAP si trova in una AWS Local Zone, perché l'accesso ai bucket Amazon S3 al di fuori della Local Zone comporta una latenza maggiore e influisce sulle attività di Cloud Volumes ONTAP.

Dimensione del disco EBS

Se si sceglie una configurazione che non supporta il"Funzionalità Amazon EBS Elastic Volumes" , è necessario scegliere una dimensione iniziale del disco quando si avvia un sistema Cloud Volumes ONTAP . Dopo di che puoi"lascia che la Console gestisca la capacità di un sistema per te" , ma se vuoi"crea aggregati tu stesso" , tieni presente quanto segue:

- Tutti i dischi di un aggregato devono avere le stesse dimensioni.
- Le prestazioni dei dischi EBS sono legate alle dimensioni del disco. La dimensione determina gli IOPS di base e la durata massima del burst per i dischi SSD e la velocità effettiva di base e di burst per i dischi HDD.
- In definitiva, dovresti scegliere la dimensione del disco che ti garantisce le *prestazioni sostenute* di cui hai bisogno.
- Anche se si scelgono dischi più grandi (ad esempio, sei dischi da 4 TiB), è possibile che non si ottengano tutti gli IOPS perché l'istanza EC2 potrebbe raggiungere il limite di larghezza di banda.

  Per maggiori dettagli sulle prestazioni del disco EBS, fare riferimento a "Documentazione AWS: Tipi di volume EBS" .

  Come indicato in precedenza, la scelta della dimensione del disco non è supportata con le configurazioni Cloud Volumes ONTAP che supportano la funzionalità Amazon EBS Elastic Volumes. "Scopri di più sul supporto di Elastic Volumes" .

Visualizza i dischi di sistema predefiniti

Oltre allo storage per i dati utente, la Console acquista anche storage cloud per i dati di sistema Cloud Volumes ONTAP (dati di avvio, dati root, dati core e NVRAM). Ai fini della pianificazione, potrebbe essere utile rivedere questi dettagli prima di distribuire Cloud Volumes ONTAP.

"Visualizza i dischi predefiniti per i dati di sistema Cloud Volumes ONTAP in AWS" .

L'agente Console richiede anche un disco di sistema. "Visualizza i dettagli sulla configurazione predefinita dell'agente della console" .

Preparati a distribuire Cloud Volumes ONTAP in un AWS Outpost

Se disponi di un AWS Outpost, puoi distribuire Cloud Volumes ONTAP in quell'Outpost selezionando l'Outpost VPC durante il processo di distribuzione. L'esperienza è la stessa di qualsiasi altra VPC residente in AWS. Tieni presente che dovrai prima distribuire un agente Console nel tuo AWS Outpost.

Ci sono alcune limitazioni da sottolineare:

- Al momento sono supportati solo i sistemi Cloud Volumes ONTAP a nodo singolo
- Le istanze EC2 che puoi utilizzare con Cloud Volumes ONTAP sono limitate a quelle disponibili nel tuo Outpost
- Al momento sono supportati solo gli SSD General Purpose (gp2)

Raccogliere informazioni di rete

Quando avvii Cloud Volumes ONTAP in AWS, devi specificare i dettagli sulla tua rete VPC. Puoi utilizzare un foglio di lavoro per raccogliere le informazioni dal tuo amministratore.

Singolo nodo o coppia HA in una singola AZ

Informazioni AWS	Il tuo valore
Regione	
VPC	
Sottorete	
Gruppo di sicurezza (se ne utilizzi uno tuo)	

Coppia HA in più AZ

Informazioni AWS	Il tuo valore
Regione	
VPC	
Gruppo di sicurezza (se ne utilizzi uno tuo)	
Zona di disponibilità del nodo 1	
Sottorete del nodo 1	
Zona di disponibilità del nodo 2	
Sottorete del nodo 2	
Zona di disponibilità del mediatore	
Sottorete mediatrice	
Coppia di chiavi per il mediatore	
Indirizzo IP mobile per la porta di gestione del cluster	
Indirizzo IP mobile per i dati sul nodo 1	
Indirizzo IP mobile per i dati sul nodo 2	
Tabelle di routing per indirizzi IP mobili	

Scegli una velocità di scrittura

La console consente di scegliere un'impostazione della velocità di scrittura per Cloud Volumes ONTAP. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normale e alta, nonché i rischi e i consigli relativi all'utilizzo di una velocità di scrittura elevata. "Scopri di più sulla velocità di

scrittura" .

Scegli un profilo di utilizzo del volume

ONTAP include diverse funzionalità di efficienza di archiviazione che possono ridurre la quantità totale di spazio di archiviazione necessario. Quando si crea un volume nella Console, è possibile scegliere un profilo che abiliti queste funzionalità oppure un profilo che le disabiliti. Dovresti saperne di più su queste funzionalità per decidere quale profilo utilizzare.

Le funzionalità di efficienza dello storage NetApp offrono i seguenti vantaggi:

Provisioning sottile
: Offre agli host o agli utenti più spazio di archiviazione logica di quello effettivamente disponibile nel pool di archiviazione fisico. Invece di preallocare lo spazio di archiviazione, lo spazio di archiviazione viene allocato dinamicamente a ciascun volume man mano che i dati vengono scritti.

Deduplicazione
: Migliora l'efficienza individuando blocchi di dati identici e sostituendoli con riferimenti a un singolo blocco condiviso. Questa tecnica riduce i requisiti di capacità di archiviazione eliminando i blocchi ridondanti di dati che risiedono nello stesso volume.

Compressione
: Riduce la capacità fisica necessaria per archiviare i dati comprimendoli all'interno di un volume su storage primario, secondario e di archivio.

Configura la tua rete

Configurare la rete AWS per Cloud Volumes ONTAP

La NetApp Console gestisce la configurazione dei componenti di rete per Cloud Volumes ONTAP, come indirizzi IP, maschere di rete e percorsi. È necessario assicurarsi che l'accesso a Internet in uscita sia disponibile, che siano disponibili sufficienti indirizzi IP privati, che siano attive le connessioni giuste e altro ancora.

Requisiti generali

Assicurati di aver soddisfatto i seguenti requisiti in AWS.

Accesso Internet in uscita per i nodi Cloud Volumes ONTAP

I sistemi Cloud Volumes ONTAP necessitano di accesso a Internet in uscita per accedere agli endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con requisiti di sicurezza rigorosi.

L'agente della console contatta diversi endpoint per le operazioni quotidiane. Per informazioni sugli endpoint utilizzati, fare riferimento a "Visualizza gli endpoint contattati dall'agente della console" E "Preparare la rete per l'utilizzo della console" .

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se l'endpoint non è disponibile
\ https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione nella Console.	Modalità standard e limitata.	L'autenticazione dell'utente fallisce e i seguenti servizi rimangono non disponibili: • Servizi Cloud Volumes ONTAP • Servizi ONTAP • Protocolli e servizi proxy
\ https://api.bluexp.netapp.com/tenancy	Locazione	Utilizzato per recuperare la risorsa Cloud Volumes ONTAP dalla Console per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilizzato per inviare i dati di telemetria AutoSupport al supporto NetApp .	Modalità standard e limitata.	Le informazioni AutoSupport non vengono recapitate.
L'endpoint commerciale esatto per il servizio AWS (con suffisso `amazonaws.com`) dipende dalla regione AWS che stai utilizzando. Fare riferimento al "Documentazione AWS per i dettagli" .	• Formazione delle nuvole • Elastic Compute Cloud (EC2) • Gestione dell'identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • Amazon Simple Storage Service (S3)	Comunicazione con i servizi AWS.	Modalità standard e privata.	Cloud Volumes ONTAP non è in grado di comunicare con il servizio AWS per eseguire operazioni specifiche in AWS.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se l'endpoint non è disponibile
L'endpoint governativo esatto per il servizio AWS dipende dalla regione AWS utilizzata. Gli endpoint sono suffissi con `amazonaws.com` E `c2s.ic.gov` . Fare riferimento a "Kit di sviluppo software AWS" E "Documentazione AWS" per maggiori informazioni.	• Formazione delle nuvole • Elastic Compute Cloud (EC2) • Gestione dell'identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • Servizio di archiviazione semplice (S3)	Comunicazione con i servizi AWS.	Modalità limitata.	Cloud Volumes ONTAP non è in grado di comunicare con il servizio AWS per eseguire operazioni specifiche in AWS.

Accesso Internet in uscita per il mediatore HA

L'istanza del mediatore HA deve disporre di una connessione in uscita al servizio AWS EC2 per poter supportare il failover dell'archiviazione. Per fornire la connessione, è possibile aggiungere un indirizzo IP pubblico, specificare un server proxy o utilizzare un'opzione manuale.

L'opzione manuale può essere un gateway NAT o un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2. Per i dettagli sugli endpoint VPC, fare riferimento a "Documentazione AWS: Endpoint VPC dell'interfaccia (AWS PrivateLink)" .

Configurazione del proxy di rete dell'agente NetApp Console

È possibile utilizzare la configurazione dei server proxy dell'agente NetApp Console per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. La console supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy dell'agente della console. L'amministratore potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato sul sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.
- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP tramite il proxy per l'agente della console. Quando si configura un proxy trasparente, l'amministratore deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurati di ottenere e caricare lo stesso certificato CA radice sul tuo sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy, fare riferimento a "Configurare l'agente della console per utilizzare un server proxy" .

Indirizzi IP privati

La console assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP. È necessario assicurarsi che la rete disponga di un numero sufficiente di indirizzi IP privati.

Il numero di LIF che la Console assegna per Cloud Volumes ONTAP dipende dal fatto che si distribuisca un sistema a nodo singolo o una coppia HA. Un LIF è un indirizzo IP associato a una porta fisica.

Indirizzi IP per un sistema a nodo singolo

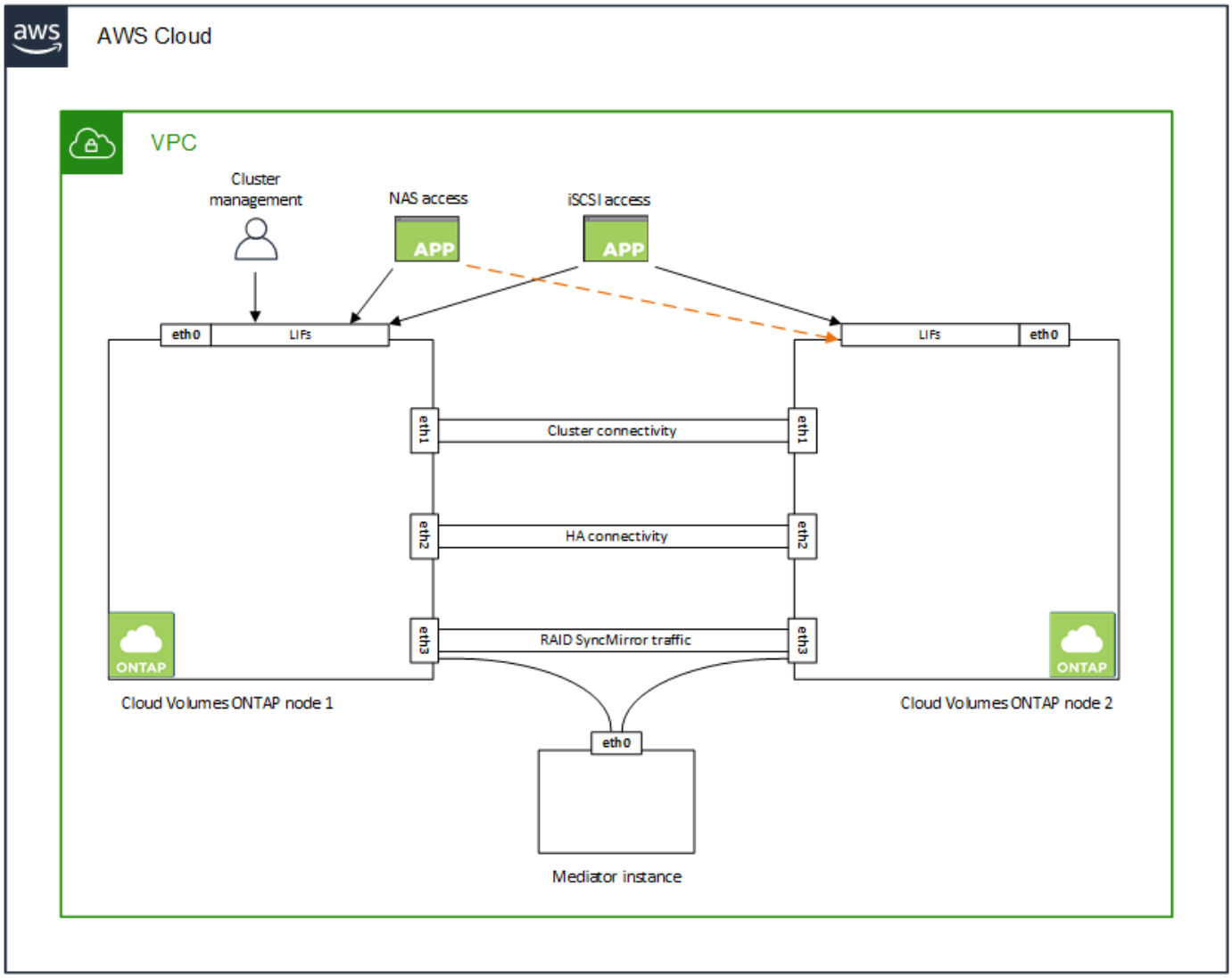
La NetApp Console assegna 6 indirizzi IP a un sistema a nodo singolo.

La tabella seguente fornisce dettagli sui LIF associati a ciascun indirizzo IP privato.

VITA	Scopo
Gestione dei cluster	Gestione amministrativa dell'intero cluster (coppia HA).
Gestione dei nodi	Gestione amministrativa di un nodo.
Intercluster	Comunicazione, backup e replica tra cluster.
Dati NAS	Accesso client tramite protocolli NAS.
dati iSCSI	Accesso client tramite protocollo iSCSI. Utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questo LIF è obbligatorio e non deve essere eliminato.
Gestione delle VM di archiviazione	Un LIF di gestione delle VM di storage viene utilizzato con strumenti di gestione come SnapCenter.

Indirizzi IP per coppie HA

Le coppie HA richiedono più indirizzi IP rispetto a un sistema a nodo singolo. Questi indirizzi IP sono distribuiti su diverse interfacce ethernet, come mostrato nell'immagine seguente:



Il numero di indirizzi IP privati richiesti per una coppia HA dipende dal modello di distribuzione scelto. Una coppia HA distribuita in una *singola* zona di disponibilità (AZ) AWS richiede 15 indirizzi IP privati, mentre una coppia HA distribuita in *più* AZ richiede 13 indirizzi IP privati.

Le tabelle seguenti forniscono dettagli sui LIF associati a ciascun indirizzo IP privato.

VITA	Interfaccia	Nodo	Scopo
Gestione dei cluster	eth0	nodo 1	Gestione amministrativa dell'intero cluster (coppia HA).
Gestione dei nodi	eth0	nodo 1 e nodo 2	Gestione amministrativa di un nodo.
Intercluster	eth0	nodo 1 e nodo 2	Comunicazione, backup e replica tra cluster.
Dati NAS	eth0	nodo 1	Accesso client tramite protocolli NAS.
dati iSCSI	eth0	nodo 1 e nodo 2	Accesso client tramite protocollo iSCSI. Utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere eliminati.

VITA	Interfaccia	Nodo	Scopo
Connettività del cluster	eth1	nodo 1 e nodo 2	Consente ai nodi di comunicare tra loro e di spostare i dati all'interno del cluster.
Connettività HA	eth2	nodo 1 e nodo 2	Comunicazione tra i due nodi in caso di failover.
Traffico iSCSI RSM	eth3	nodo 1 e nodo 2	Traffico iSCSI RAID SyncMirror , nonché comunicazione tra i due nodi Cloud Volumes ONTAP e il mediatore.
Mediatore	eth0	Mediatore	Un canale di comunicazione tra i nodi e il mediatore per facilitare i processi di acquisizione e restituzione dello storage.

VITA	Interfaccia	Nodo	Scopo
Gestione dei nodi	eth0	nodo 1 e nodo 2	Gestione amministrativa di un nodo.
Intercluster	eth0	nodo 1 e nodo 2	Comunicazione, backup e replica tra cluster.
dati iSCSI	eth0	nodo 1 e nodo 2	Accesso client tramite protocollo iSCSI. Questi LIF gestiscono anche la migrazione degli indirizzi IP flottanti tra i nodi. Questi LIF sono obbligatori e non devono essere eliminati.
Connettività del cluster	eth1	nodo 1 e nodo 2	Consente ai nodi di comunicare tra loro e di spostare i dati all'interno del cluster.
Connettività HA	eth2	nodo 1 e nodo 2	Comunicazione tra i due nodi in caso di failover.
Traffico iSCSI RSM	eth3	nodo 1 e nodo 2	Traffico iSCSI RAID SyncMirror , nonché comunicazione tra i due nodi Cloud Volumes ONTAP e il mediatore.
Mediatore	eth0	Mediatore	Un canale di comunicazione tra i nodi e il mediatore per facilitare i processi di acquisizione e restituzione dello storage.

Quando distribuiti in più zone di disponibilità, diversi LIF sono associati a"indirizzi IP flottanti" , che non vengono conteggiati nel limite IP privato di AWS.

Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché la Console lo fa per te. Se devi usare il tuo, fai riferimento a"Regole del gruppo di sicurezza" .

Cerchi informazioni sull'agente Console? "Visualizza le regole del gruppo di sicurezza per l'agente della console"

Connessione per la suddivisione in livelli dei dati

Se si desidera utilizzare EBS come livello di prestazioni e Amazon S3 come livello di capacità, è necessario assicurarsi che Cloud Volumes ONTAP disponga di una connessione a S3. Il modo migliore per fornire tale connessione è creare un VPC Endpoint per il servizio S3. Per istruzioni, consultare il "Documentazione AWS: creazione di un endpoint gateway".

Quando crei l'endpoint VPC, assicurati di selezionare la regione, la VPC e la tabella di routing che corrispondono all'istanza Cloud Volumes ONTAP . È inoltre necessario modificare il gruppo di sicurezza per aggiungere una regola HTTPS in uscita che consenta il traffico verso l'endpoint S3. In caso contrario, Cloud Volumes ONTAP non potrà connettersi al servizio S3.

Se riscontri problemi, fai riferimento a "AWS Support Knowledge Center: perché non riesco a connettermi a un bucket S3 tramite un endpoint VPC gateway?"

Collegamenti ai sistemi ONTAP

Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra AWS VPC e l'altra rete, ad esempio la rete aziendale. Per le istruzioni, fare riferimento al "Documentazione AWS: configurazione di una connessione VPN AWS" .

DNS e Active Directory per CIFS

Se si desidera eseguire il provisioning di storage CIFS, è necessario configurare DNS e Active Directory in AWS oppure estendere la configurazione locale ad AWS.

Il server DNS deve fornire servizi di risoluzione dei nomi per l'ambiente Active Directory. È possibile configurare i set di opzioni DHCP in modo che utilizzino il server DNS EC2 predefinito, che non deve essere il server DNS utilizzato dall'ambiente Active Directory.

Per le istruzioni, fare riferimento al "Documentazione AWS: Servizi di dominio Active Directory sul cloud AWS: distribuzione di riferimento rapido" .

Condivisione VPC

A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP HA sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere subnet con altri account AWS. Per utilizzare questa configurazione, è necessario impostare l'ambiente AWS e quindi distribuire la coppia HA tramite l'API.

"Scopri come distribuire una coppia HA in una subnet condivisa" .

Requisiti per coppie HA in più AZ

Ulteriori requisiti di rete AWS si applicano alle configurazioni Cloud Volumes ONTAP HA che utilizzano più zone di disponibilità (AZ). È opportuno esaminare questi requisiti prima di avviare una coppia HA, poiché è necessario immettere i dettagli di rete nella Console quando si aggiunge un sistema Cloud Volumes ONTAP .

Per comprendere come funzionano le coppie HA, fare riferimento a"Coppie ad alta disponibilità" .

Zone di disponibilità

Questo modello di distribuzione HA utilizza più AZ per garantire un'elevata disponibilità dei dati. È necessario utilizzare una AZ dedicata per ogni istanza Cloud Volumes ONTAP e per l'istanza mediatrice, che fornisce un canale di comunicazione tra la coppia HA.

In ogni zona di disponibilità dovrebbe essere disponibile una subnet.

Indirizzi IP flottanti per dati NAS e gestione cluster/SVM

Le configurazioni HA in più AZ utilizzano indirizzi IP mobili che migrano tra i nodi in caso di guasti. Non sono accessibili in modo nativo dall'esterno della VPC, a meno che tu non"configurare un gateway di transito AWS" .

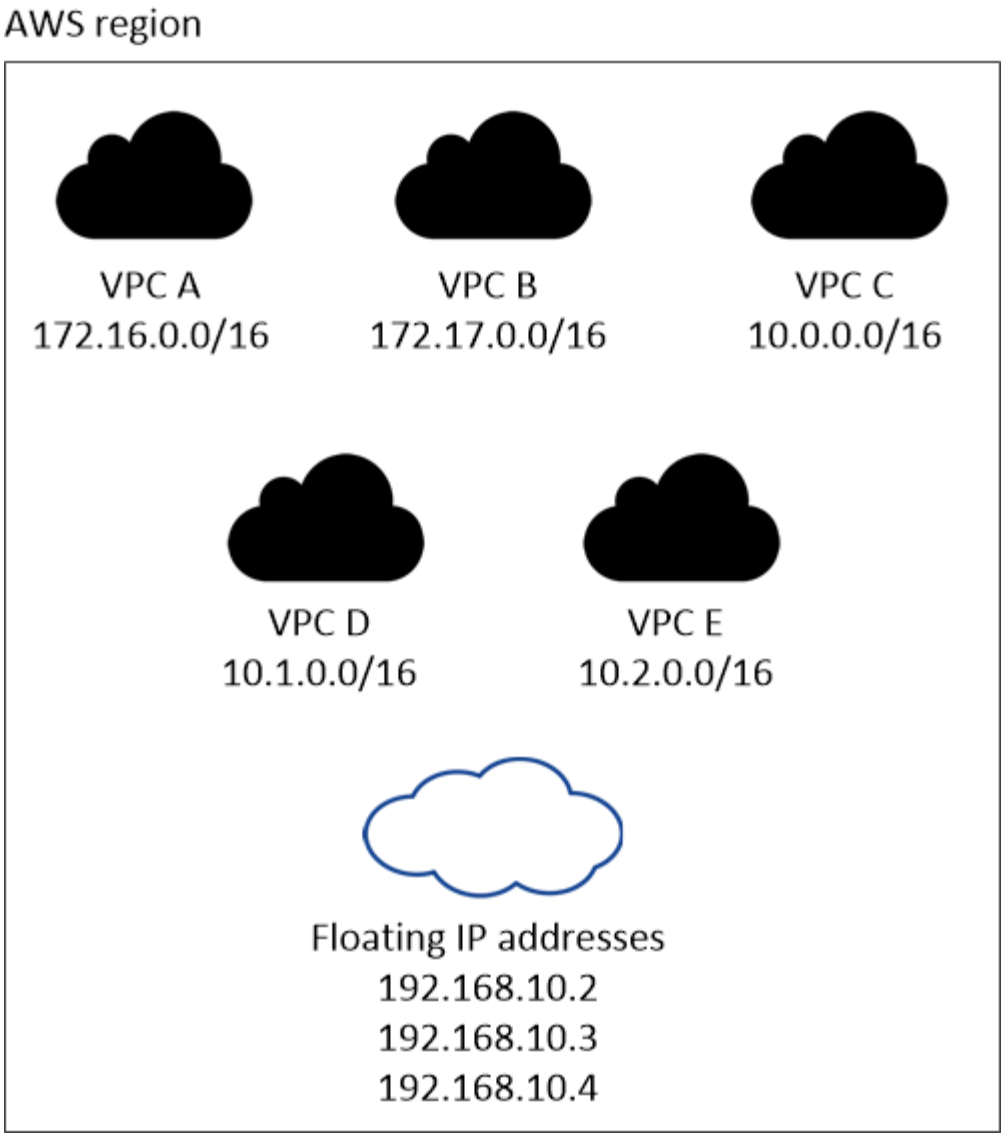
Un indirizzo IP mobile è per la gestione del cluster, uno è per i dati NFS/CIFS sul nodo 1 e uno è per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è facoltativo.

Se si utilizza SnapDrive per Windows o SnapCenter con la coppia HA, è necessario un indirizzo IP mobile per la gestione SVM LIF.

Quando si aggiunge un sistema Cloud Volumes ONTAP HA, è necessario immettere gli indirizzi IP mobili. La console assegna gli indirizzi IP alla coppia HA quando avvia il sistema.

Gli indirizzi IP mobili devono essere esterni ai blocchi CIDR per tutte le VPC nella regione AWS in cui si distribuisce la configurazione HA. Considera gli indirizzi IP mobili come una subnet logica esterna alle VPC nella tua regione.

L'esempio seguente mostra la relazione tra indirizzi IP mobili e VPC in una regione AWS. Sebbene gli indirizzi IP mobili siano al di fuori dei blocchi CIDR per tutte le VPC, sono instradabili verso le subnet tramite tabelle di routing.



La console crea automaticamente indirizzi IP statici per l'accesso iSCSI e per l'accesso NAS da client esterni alla VPC. Per questi tipi di indirizzi IP non è necessario soddisfare alcun requisito.

Gateway di transito per abilitare l'accesso IP flottante dall'esterno della VPC

Se necessario,"configurare un gateway di transito AWS" per consentire l'accesso agli indirizzi IP mobili di una coppia HA dall'esterno della VPC in cui risiede la coppia HA.

Tabelle di routing

Dopo aver specificato gli indirizzi IP mobili, ti verrà chiesto di selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili. Ciò consente al client di accedere alla coppia HA.

Se si dispone di una sola tabella di routing per le subnet nella VPC (la tabella di routing principale), la Console aggiunge automaticamente gli indirizzi IP mobili a tale tabella di routing. Se si dispone di più di una tabella di routing, è molto importante selezionare le tabelle di routing corrette quando si avvia la coppia HA. In caso contrario, alcuni client potrebbero non avere accesso a Cloud Volumes ONTAP.

Ad esempio, potresti avere due subnet associate a tabelle di routing diverse. Se si seleziona la tabella di routing A, ma non la tabella di routing B, i client nella subnet associata alla tabella di routing A possono

accedere alla coppia HA, ma i client nella subnet associata alla tabella di routing B non possono.

Per ulteriori informazioni sulle tabelle di routing, fare riferimento a "Documentazione AWS: tabelle di routing" .

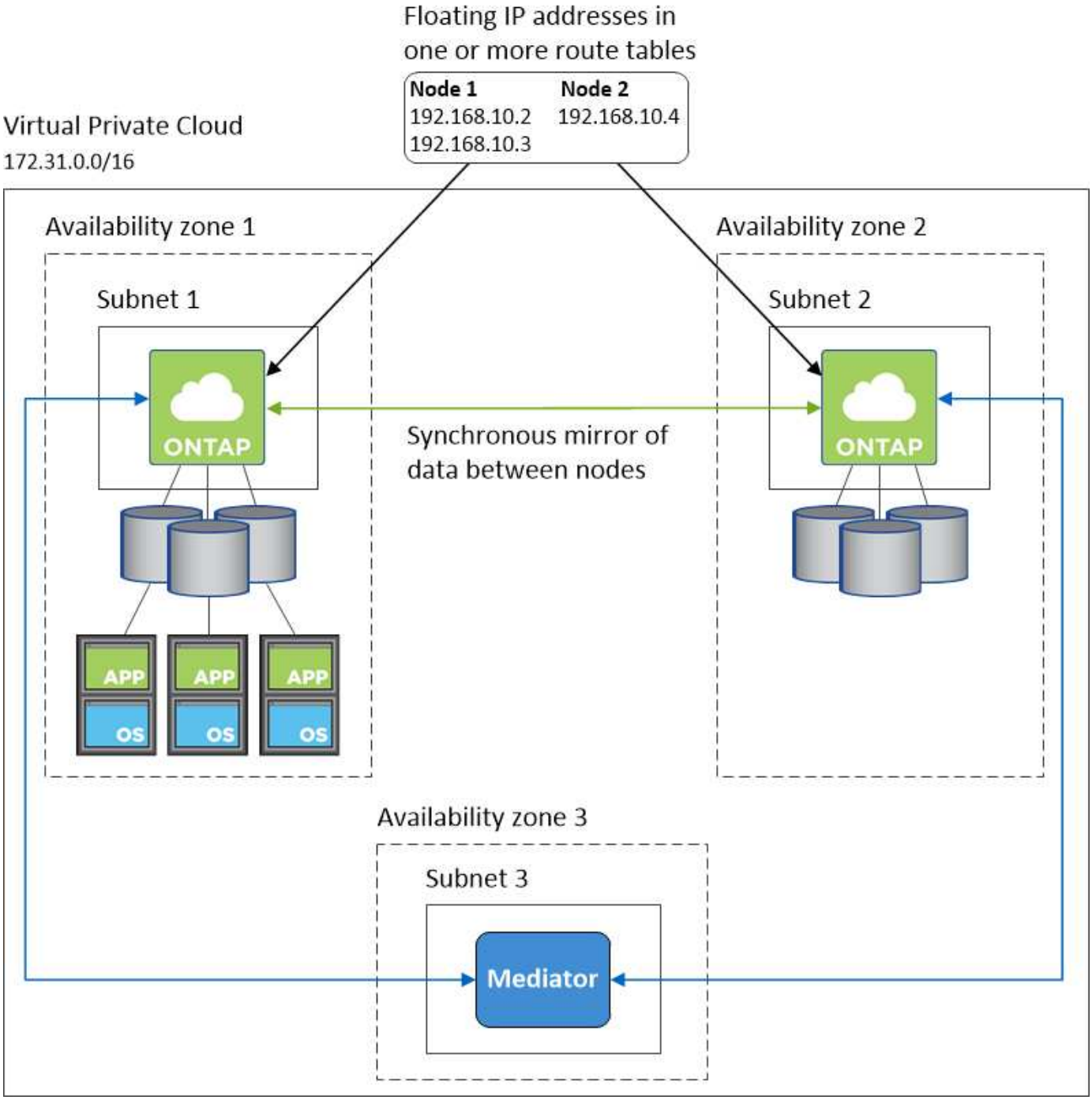
Connessione agli strumenti di gestione NetApp

Per utilizzare gli strumenti di gestione NetApp con configurazioni HA presenti in più AZ, sono disponibili due opzioni di connessione:

1. Distribuire gli strumenti di gestione NetApp in una VPC diversa e"configurare un gateway di transito AWS" . Il gateway consente l'accesso all'indirizzo IP flottante per l'interfaccia di gestione del cluster dall'esterno della VPC.
2. Distribuire gli strumenti di gestione NetApp nella stessa VPC con una configurazione di routing simile a quella dei client NAS.

Esempio di configurazione HA

L'immagine seguente illustra i componenti di rete specifici di una coppia HA in più AZ: tre zone di disponibilità, tre subnet, indirizzi IP mobili e una tabella di routing.



Requisiti per l'agente della console

Se non hai ancora creato un agente Console, dovresti rivedere i requisiti di rete.

- "Visualizza i requisiti di rete per l'agente della console"
- "Regole del gruppo di sicurezza in AWS"

Argomenti correlati

- "Verifica la configurazione AutoSupport per Cloud Volumes ONTAP"
- "Scopri di più sulle porte interne ONTAP" .

Configurare un gateway di transito AWS per coppie Cloud Volumes ONTAP HA

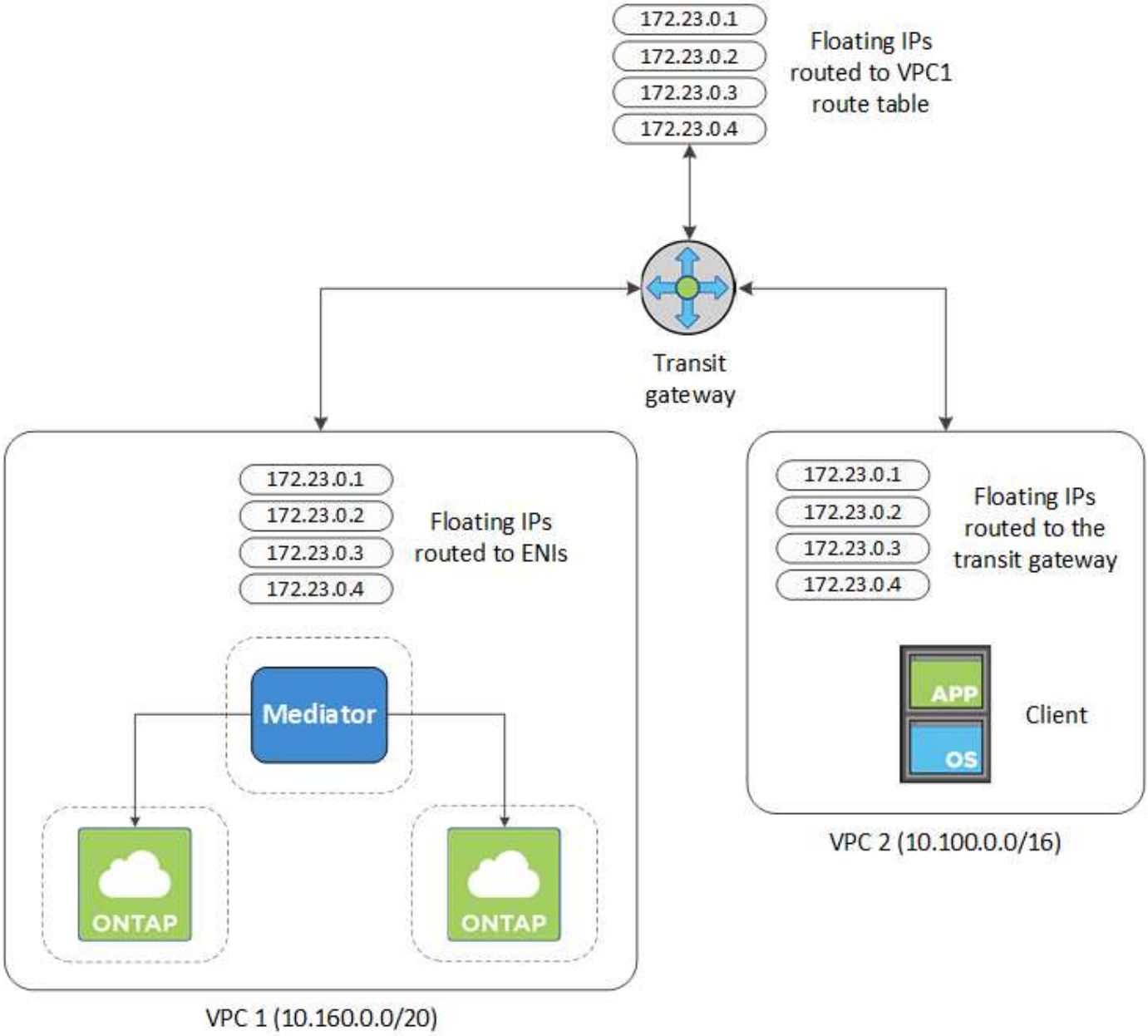
Impostare un gateway di transito AWS per abilitare l'accesso a una coppia HA"indirizzi IP flottanti" dall'esterno della VPC in cui risiede la coppia HA.

Quando una configurazione Cloud Volumes ONTAP HA è distribuita su più zone di disponibilità AWS, sono necessari indirizzi IP mobili per l'accesso ai dati NAS dall'interno della VPC. Questi indirizzi IP mobili possono migrare tra i nodi in caso di guasti, ma non sono accessibili in modo nativo dall'esterno della VPC. Indirizzi IP privati separati forniscono l'accesso ai dati dall'esterno della VPC, ma non forniscono il failover automatico.

Sono richiesti anche indirizzi IP flottanti per l'interfaccia di gestione del cluster e per il LIF di gestione SVM opzionale.

Se si configura un gateway di transito AWS, si abilita l'accesso agli indirizzi IP mobili dall'esterno della VPC in cui risiede la coppia HA. Ciò significa che i client NAS e gli strumenti di gestione NetApp esterni alla VPC possono accedere agli IP mobili.

Ecco un esempio che mostra due VPC connesse tramite un gateway di transito. Un sistema HA risiede in una VPC, mentre un client risiede nell'altra. È quindi possibile montare un volume NAS sul client utilizzando l'indirizzo IP flottante.

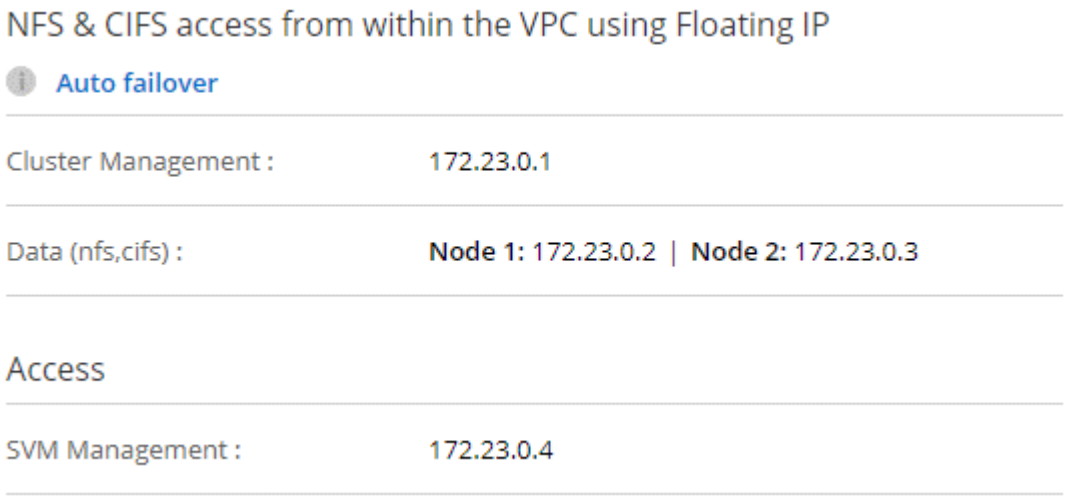


I passaggi seguenti illustrano come impostare una configurazione simile.

Passi

1. "Creare un gateway di transito e collegare le VPC al gateway" .
2. Associare le VPC alla tabella di routing del gateway di transito.
   a. Nel servizio **VPC**, fare clic su **Tabelle di routing del gateway di transito**.
   b. Selezionare la tabella di routing.
   c. Fare clic su **Associazioni** e quindi selezionare **Crea associazione**.
   d. Selezionare gli allegati (VPC) da associare, quindi fare clic su **Crea associazione**.
3. Creare percorsi nella tabella di routing del gateway di transito specificando gli indirizzi IP flottanti della coppia HA.

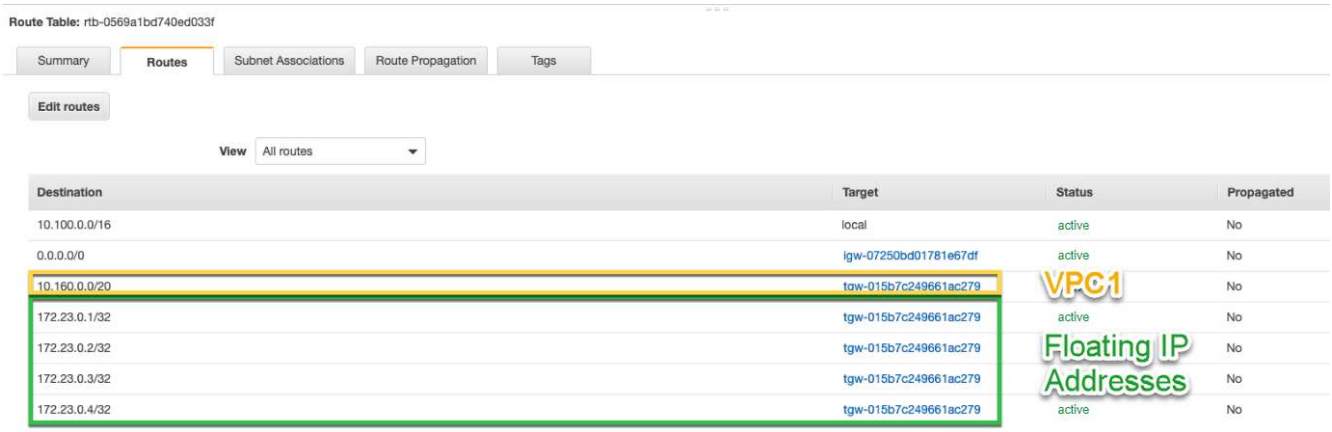
   Puoi trovare gli indirizzi IP mobili nella pagina delle informazioni di sistema nella NetApp Console. Ecco un esempio:



L'immagine di esempio seguente mostra la tabella di routing per il gateway di transito. Include percorsi verso i blocchi CIDR delle due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

4. Modificare la tabella di routing delle VPC che devono accedere agli indirizzi IP mobili.
   a. Aggiungere voci di percorso agli indirizzi IP mobili.
   b. Aggiungere una voce di percorso al blocco CIDR della VPC in cui risiede la coppia HA.

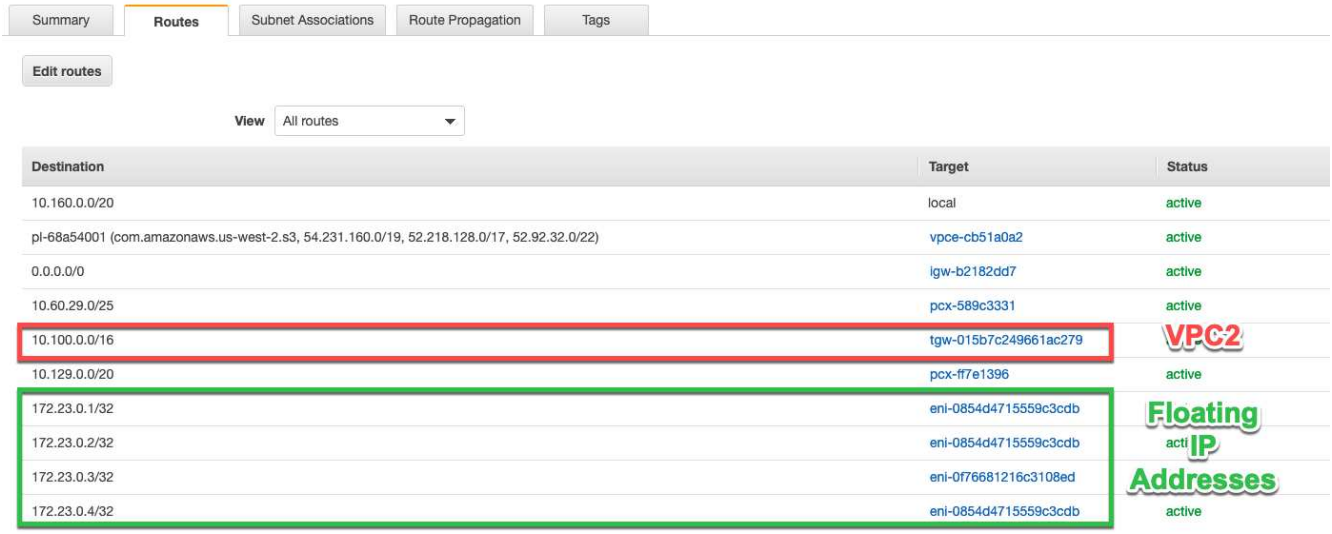
      L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



5. Modificare la tabella di routing per la VPC della coppia HA aggiungendo una route alla VPC che necessita di accesso agli indirizzi IP flottanti.

   Questo passaggio è importante perché completa il routing tra le VPC.

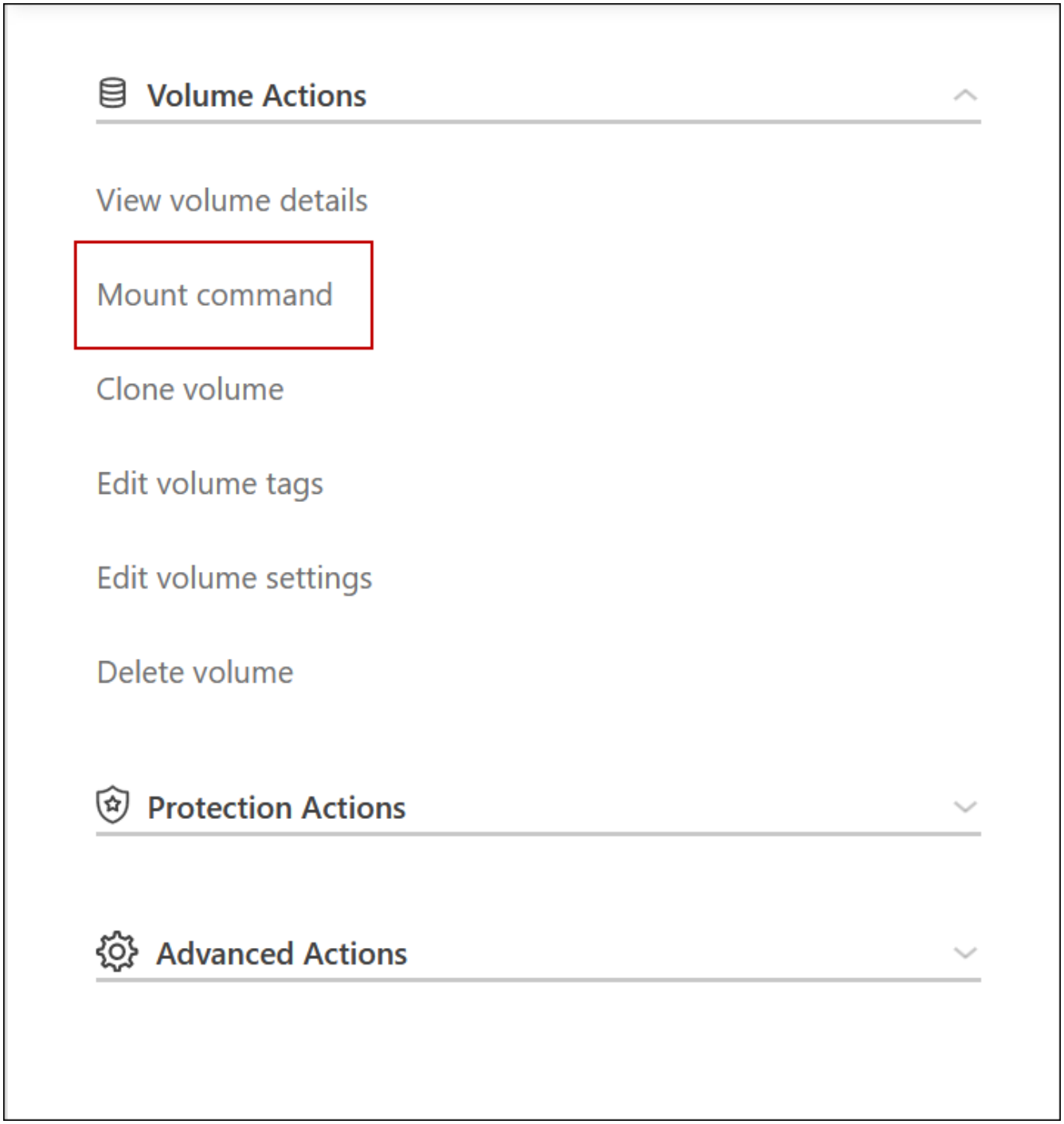
   L'immagine di esempio seguente mostra la tabella di routing per VPC 1. Include un percorso verso gli indirizzi IP mobili e verso VPC 2, dove risiede un client. La console ha aggiunto automaticamente gli IP mobili alla tabella di routing quando ha distribuito la coppia HA.



6. Aggiorna le impostazioni dei gruppi di sicurezza su Tutto il traffico per la VPC.
   a. In Virtual Private Cloud, fare clic su **Sottoreti**.
   b. Fare clic sulla scheda **Tabella di routing** e selezionare l'ambiente desiderato per uno degli indirizzi IP mobili per una coppia HA.
   c. Fare clic su **Gruppi di sicurezza**.
   d. Selezionare **Modifica regole in entrata**.
   e. Fare clic su **Aggiungi regola**.
   f. In Tipo, seleziona **Tutto il traffico**, quindi seleziona l'indirizzo IP VPC.
   g. Fare clic su **Salva regole** per applicare le modifiche.
7. Montare i volumi sui client utilizzando l'indirizzo IP mobile.

   È possibile trovare l'indirizzo IP corretto nella Console tramite l'opzione **Comando di montaggio** nel

pannello Gestisci volumi nella Console.



8. Se si sta montando un volume NFS, configurare la policy di esportazione in modo che corrisponda alla subnet del VPC client.

   "Scopri come modificare un volume" .

Link correlati

- "Coppie ad alta disponibilità in AWS"
- "Requisiti di rete per Cloud Volumes ONTAP in AWS"

Distribuisci coppie Cloud Volumes ONTAP HA in una subnet condivisa AWS

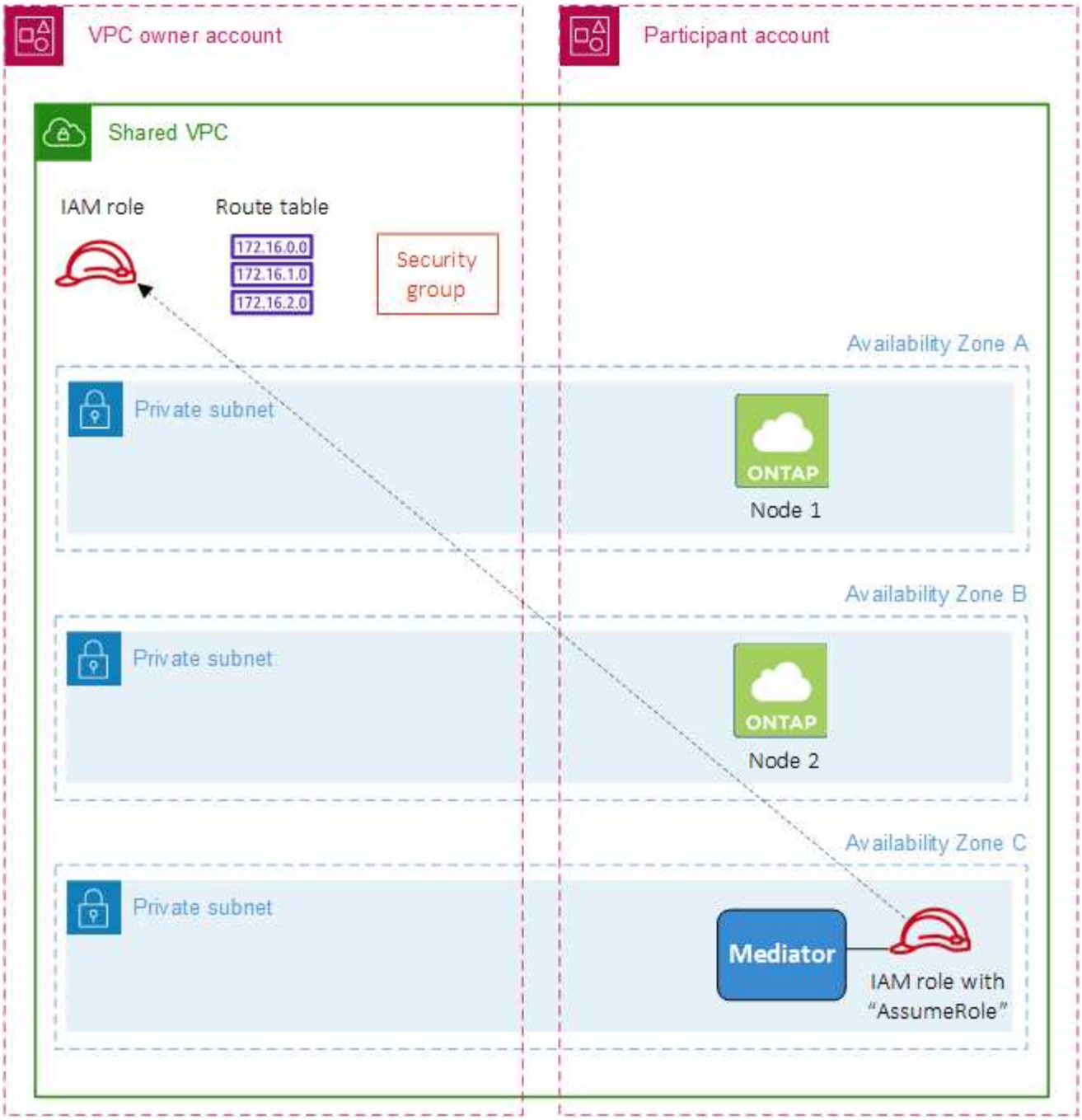
A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP HA sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere subnet con altri account AWS. Per utilizzare questa configurazione, è necessario impostare l'ambiente AWS e quindi distribuire la coppia HA tramite l'API.

Con "Condivisione VPC" , una configurazione Cloud Volumes ONTAP HA è distribuita su due account:

- L'account proprietario della VPC, che possiede la rete (la VPC, le subnet, le tabelle di routing e il gruppo di sicurezza Cloud Volumes ONTAP)
- L'account del partecipante, in cui le istanze EC2 vengono distribuite in subnet condivise (inclusi i due nodi HA e il mediatore)

Nel caso di una configurazione Cloud Volumes ONTAP HA distribuita su più zone di disponibilità, il mediatore HA necessita di autorizzazioni specifiche per scrivere nelle tabelle di routing nell'account proprietario della VPC. È necessario fornire tali autorizzazioni impostando un ruolo IAM che il mediatore può assumere.

L'immagine seguente mostra i componenti coinvolti in questa distribuzione:



Come descritto nei passaggi seguenti, dovrai condividere le subnet con l'account del partecipante e quindi creare il ruolo IAM e il gruppo di sicurezza nell'account del proprietario della VPC.

Quando si crea il sistema Cloud Volumes ONTAP , la NetApp Console crea automaticamente e associa un ruolo IAM al mediatore. Questo ruolo assume il ruolo IAM creato nell'account proprietario VPC per apportare modifiche alle tabelle di routing associate alla coppia HA.

Passi

1. Condividere le subnet nell'account proprietario della VPC con l'account partecipante.

   Questo passaggio è necessario per distribuire la coppia HA in subnet condivise.

   "Documentazione AWS: condividere una sottorete"

2. Nell'account proprietario VPC, creare un gruppo di sicurezza per Cloud Volumes ONTAP.

   "Fare riferimento alle regole del gruppo di sicurezza per Cloud Volumes ONTAP" . Tieni presente che non è necessario creare un gruppo di sicurezza per il mediatore HA. La Console lo fa per te.

3. Nell'account proprietario della VPC, crea un ruolo IAM che includa le seguenti autorizzazioni:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Utilizzare l'API per creare un nuovo sistema Cloud Volumes ONTAP .

   Si noti che è necessario specificare i seguenti campi:

   - "securityGroupId"

     Il campo "securityGroupId" deve specificare il gruppo di sicurezza creato nell'account proprietario della VPC (vedere il passaggio 2 sopra).

   - "assumeRoleArn" nell'oggetto "haParams"

     Il campo "assumeRoleArn" deve includere l'ARN del ruolo IAM creato nell'account proprietario della VPC (vedere il passaggio 3 sopra).

     Per esempio:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Scopri di più sull'API Cloud Volumes ONTAP"

Configurare la creazione di gruppi di posizionamento per coppie Cloud Volumes ONTAP HA nelle singole zone di disponibilità AWS

Le distribuzioni ad alta disponibilità (HA) Cloud Volumes ONTAP nella zona di disponibilità singola (AZ) di AWS possono non riuscire e subire il rollback se la creazione del gruppo di posizionamento non riesce. Anche la creazione del gruppo di posizionamento fallisce e la distribuzione viene annullata se il nodo Cloud Volumes

ONTAP e l'istanza del mediatore non sono disponibili. Per evitare questo problema, è possibile modificare la configurazione per consentire il completamento della distribuzione anche se la creazione del gruppo di posizionamento non riesce.

Se si ignora il processo di rollback, il processo di distribuzione Cloud Volumes ONTAP viene completato correttamente e viene notificato che la creazione del gruppo di posizionamento non è completa.

Passi

1. Utilizzare SSH per connettersi all'host dell'agente NetApp Console ed effettuare l'accesso.
2. Vai a `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. Modificare `app.conf` modificando il valore del `rollback-on-placement-group-failure` parametro a `false` . Il valore predefinito di questo parametro è `true` .

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Salvare il file e disconnettersi dall'agente della console. Non è necessario riavviare l'agente Console.

Regole in entrata e in uscita del gruppo di sicurezza AWS per Cloud Volumes ONTAP

La NetApp Console crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. Potresti voler fare riferimento alle porte per scopi di test o se preferisci utilizzare i tuoi gruppi di sicurezza.

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole in entrata

Quando aggiungi un sistema Cloud Volumes ONTAP e scegli un gruppo di sicurezza predefinito, puoi scegliere di consentire il traffico all'interno di uno dei seguenti:

- **Solo VPC selezionata**: l'origine del traffico in entrata è l'intervallo di subnet della VPC per il sistema Cloud Volumes ONTAP e l'intervallo di subnet della VPC in cui risiede l'agente della console. Questa è l'opzione consigliata.
- **Tutte le VPC**: la sorgente del traffico in entrata è l'intervallo IP 0.0.0.0/0.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di ONTAP System Manager tramite l'indirizzo IP del LIF di gestione del cluster
HTTPS	443	Connettività con l'agente Console e accesso HTTPS alla console Web ONTAP System Manager utilizzando l'indirizzo IP del LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione del nodo
TCP	111	Chiamata di procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo semplice di gestione della rete
TCP	445	Microsoft SMB/CIFS su TCP con framing NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Demone del server NFS
TCP	3260	Accesso iSCSI tramite i dati iSCSI LIF
TCP	4045	Demone di blocco NFS
TCP	4046	Monitoraggio dello stato di rete per NFS
TCP	10000	Backup tramite NDMP
TCP	11104	Gestione delle sessioni di comunicazione intercluster per SnapMirror
TCP	11105	Trasferimento dati SnapMirror tramite LIF intercluster
UDP	111	Chiamata di procedura remota per NFS
UDP	161-162	Protocollo semplice di gestione della rete
UDP	635	Montaggio NFS
UDP	2049	Demone del server NFS
UDP	4045	Demone di blocco NFS
UDP	4046	Monitoraggio dello stato di rete per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti gli TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se hai bisogno di regole rigide per il traffico in uscita, puoi utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte di Cloud Volumes ONTAP.

La sorgente è l'interfaccia (indirizzo IP) sul sistema Cloud Volumes ONTAP .

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
Directory attiva	TCP	88	Gestione dei nodi LIF	Foresta di Active Directory	Autenticazione Kerberos V
	UDP	137	Gestione dei nodi LIF	Foresta di Active Directory	Servizio di denominazione NetBIOS
	UDP	138	Gestione dei nodi LIF	Foresta di Active Directory	Servizio datagramma NetBIOS
	TCP	139	Gestione dei nodi LIF	Foresta di Active Directory	Sessione del servizio NetBIOS
	TCP e UDP	389	Gestione dei nodi LIF	Foresta di Active Directory	LDAP
	TCP	445	Gestione dei nodi LIF	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	TCP	464	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	UDP	464	Gestione dei nodi LIF	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)
	TCP	88	Dati LIF (NFS, CIFS, iSCSI)	Foresta di Active Directory	Autenticazione Kerberos V
	UDP	137	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio di denominazione NetBIOS
	UDP	138	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio datagramma NetBIOS
	TCP	139	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Sessione del servizio NetBIOS
	TCP e UDP	389	Dati LIF (NFS, CIFS)	Foresta di Active Directory	LDAP
	TCP	445	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	TCP	464	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	UDP	464	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
AutoSupport	HTTPS	443	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	Gestione dei nodi LIF	Agente console	Invio di messaggi AutoSupport tramite un server proxy sull'agente Console, se non è disponibile una connessione Internet in uscita
Backup su S3	TCP	5010	Intercluster LIF	Backup dell'endpoint o ripristino dell'endpoint	Operazioni di backup e ripristino per la funzionalità Backup su S3
Grappolo	Tutto il traffico	Tutto il traffico	Tutti i LIF su un nodo	Tutti i LIF sull'altro nodo	Comunicazioni intercluster (solo Cloud Volumes ONTAP HA)
	TCP	3000	Gestione dei nodi LIF	Mediatore HA	Chiamate ZAPI (Cloud Volumes ONTAP HA)
	ICMP	1	Gestione dei nodi LIF	Mediatore HA	Mantieni attivo (Cloud Volumes ONTAP HA)
Backup di configurazione	HTTP	80	Gestione dei nodi LIF	http://<indirizzo-IP-agente-console>/occm/offboxconfig	Inviare i backup della configurazione all'agente della console."Documentazione ONTAP"
DHCP	UDP	68	Gestione dei nodi LIF	DHCP	Client DHCP per la prima configurazione
DHCP	UDP	67	Gestione dei nodi LIF	DHCP	server DHCP
DNS	UDP	53	Gestione dei nodi LIF e dati LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Gestione dei nodi LIF	Server di destinazione	Copia NDMP
SMTP	TCP	25	Gestione dei nodi LIF	Server di posta	Avvisi SMTP, possono essere utilizzati per AutoSupport

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
SNMP	TCP	161	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	UDP	161	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	TCP	162	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	UDP	162	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
SnapMirror	TCP	11104	Intercluster LIF	LIF intercluster ONTAP	Gestione delle sessioni di comunicazione intercluster per SnapMirror
	TCP	11105	Intercluster LIF	LIF intercluster ONTAP	Trasferimento dati SnapMirror
Registro di sistema	UDP	514	Gestione dei nodi LIF	Server Syslog	Messaggi di inoltro Syslog

Regole per il gruppo di sicurezza esterno del mediatore HA

Il gruppo di sicurezza esterno predefinito per il mediatore Cloud Volumes ONTAP HA include le seguenti regole in entrata e in uscita.

Regole in entrata

Il gruppo di sicurezza predefinito per il mediatore HA include la seguente regola in ingresso.

Protocollo	Porta	Fonte	Scopo
TCP	3000	CIDR dell'agente della console	Accesso API RESTful dall'agente Console

Regole in uscita

Il gruppo di sicurezza predefinito per il mediatore HA apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per il mediatore HA include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte del mediatore HA.

Protocollo	Porta	Destinazione	Scopo
HTTP	80	Indirizzo IP dell'agente della console sull'istanza AWS EC2	Scarica gli aggiornamenti per il mediatore
HTTPS	443	ec2.amazonaws.com	Assistenza con il failover dell'archiviazione
UDP	53	ec2.amazonaws.com	Assistenza con il failover dell'archiviazione

Invece di aprire le porte 443 e 53, è possibile creare un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2.

Regole per il gruppo di sicurezza interno della configurazione HA

Il gruppo di sicurezza interno predefinito per una configurazione Cloud Volumes ONTAP HA include le seguenti regole. Questo gruppo di sicurezza consente la comunicazione tra i nodi HA e tra il mediatore e i nodi.

La Console crea sempre questo gruppo di sicurezza. Non hai la possibilità di usare il tuo.

Regole in entrata

Il gruppo di sicurezza predefinito include le seguenti regole in entrata.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore HA e i nodi HA

Regole in uscita

Il gruppo di sicurezza predefinito include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore HA e i nodi HA

Regole per l'agente della console

"Visualizza le regole del gruppo di sicurezza per l'agente della console"

Configura Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in AWS

Se si desidera utilizzare la crittografia Amazon con Cloud Volumes ONTAP, è necessario configurare AWS Key Management Service (KMS).

Passi

1. Assicurarsi che esista una Customer Master Key (CMK) attiva.

   La CMK può essere una CMK gestita da AWS o una CMK gestita dal cliente. Può trovarsi nello stesso

account AWS di NetApp Console e Cloud Volumes ONTAP oppure in un account AWS diverso.

"Documentazione AWS: Chiavi master del cliente (CMK)"

2. Modificare la policy delle chiavi per ogni CMK aggiungendo il ruolo IAM che fornisce autorizzazioni alla Console come *utente chiave*.

   L'aggiunta del ruolo Identity and Access Management (IAM) come utente chiave fornisce alla Console le autorizzazioni per utilizzare CMK con Cloud Volumes ONTAP.

   "Documentazione AWS: modifica delle chiavi"

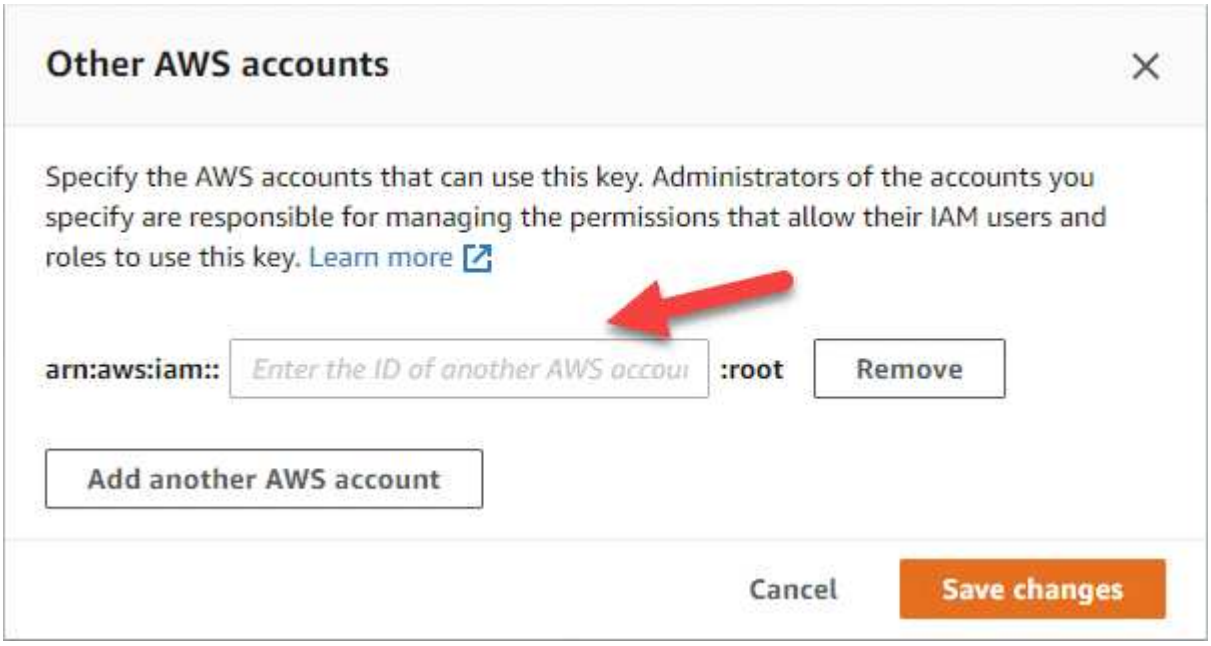
3. Se la CMK si trova in un account AWS diverso, completare i seguenti passaggi:

   a. Accedere alla console KMS dall'account in cui risiede la CMK.
   b. Selezionare la chiave.
   c. Nel riquadro **Configurazione generale**, copiare l'ARN della chiave.

      Sarà necessario fornire l'ARN alla Console quando si crea il sistema Cloud Volumes ONTAP .

   d. Nel riquadro **Altri account AWS**, aggiungi l'account AWS che fornisce le autorizzazioni alla Console.

      In genere, questo è l'account in cui viene distribuita la Console. Se la Console non è installata in AWS, utilizzare l'account per il quale sono state fornite le chiavi di accesso AWS alla Console.



e. Ora passa all'account AWS che fornisce le autorizzazioni alla Console e apri la console IAM.

f. Creare una policy IAM che includa le autorizzazioni elencate di seguito.

g. Associare il criterio al ruolo IAM o all'utente IAM che fornisce le autorizzazioni alla Console.

La seguente policy fornisce le autorizzazioni di cui la Console ha bisogno per utilizzare la CMK dall'account AWS esterno. Assicurati di modificare la regione e l'ID account nelle sezioni "Risorse".

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Per ulteriori dettagli su questo processo, fare riferimento a "Documentazione AWS: consentire agli utenti di altri account di utilizzare una chiave KMS" .

4. Se si utilizza una CMK gestita dal cliente, modificare la policy delle chiavi per la CMK aggiungendo il ruolo IAM Cloud Volumes ONTAP come *utente chiave*.

   Questo passaggio è obbligatorio se hai abilitato il tiering dei dati su Cloud Volumes ONTAP e desideri crittografare i dati archiviati nel bucket Amazon Simple Storage Service (Amazon S3).

Sarà necessario eseguire questo passaggio *dopo* aver distribuito Cloud Volumes ONTAP perché il ruolo IAM viene creato quando si crea un sistema Cloud Volumes ONTAP . (Naturalmente, hai la possibilità di utilizzare un ruolo IAM Cloud Volumes ONTAP esistente, quindi è possibile eseguire questo passaggio in anticipo.)

"Documentazione AWS: modifica delle chiavi"

Imposta i ruoli AWS IAM per i nodi Cloud Volumes ONTAP

A ciascun nodo Cloud Volumes ONTAP devono essere associati i ruoli AWS Identity and Access Management (IAM) con le autorizzazioni richieste. Lo stesso vale per il mediatore HA. È più semplice lasciare che sia la NetApp Console a creare i ruoli IAM per te, ma puoi anche utilizzare i tuoi ruoli.

Questo compito è facoltativo. Quando si crea un sistema Cloud Volumes ONTAP , l'opzione predefinita è quella di lasciare che la Console crei i ruoli IAM per conto dell'utente. Se le policy di sicurezza della tua azienda richiedono di creare autonomamente i ruoli IAM, segui i passaggi indicati di seguito.

In AWS Secret Cloud è obbligatorio fornire il proprio ruolo IAM. "Scopri come distribuire Cloud Volumes ONTAP in C2S" .

Passi

1. Vai alla console AWS IAM.
2. Creare policy IAM che includano le seguenti autorizzazioni:

   - Criterio di base per i nodi Cloud Volumes ONTAP

Regioni standard

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

Regioni GovCloud (USA)

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regioni top secret

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regioni segrete

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Criterio di backup per i nodi Cloud Volumes ONTAP

  Se si prevede di utilizzare NetApp Backup and Recovery con i sistemi Cloud Volumes ONTAP , il ruolo IAM per i nodi deve includere la seconda policy mostrata di seguito.

Regioni standard

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regioni GovCloud (USA)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regioni top secret

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regioni segrete

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- Mediatore HA

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Crea un ruolo IAM e associa i criteri creati al ruolo.

Risultato

Ora disponi di ruoli IAM che puoi selezionare quando crei un nuovo sistema Cloud Volumes ONTAP .

Ulteriori informazioni

- "Documentazione AWS: creazione di policy IAM"
- "Documentazione AWS: creazione di ruoli IAM"

Impostare le licenze per Cloud Volumes ONTAP in AWS

Dopo aver deciso quale opzione di licenza utilizzare con Cloud Volumes ONTAP, sono necessari alcuni passaggi prima di poter scegliere tale opzione di licenza durante la creazione di un nuovo sistema.

Freemium

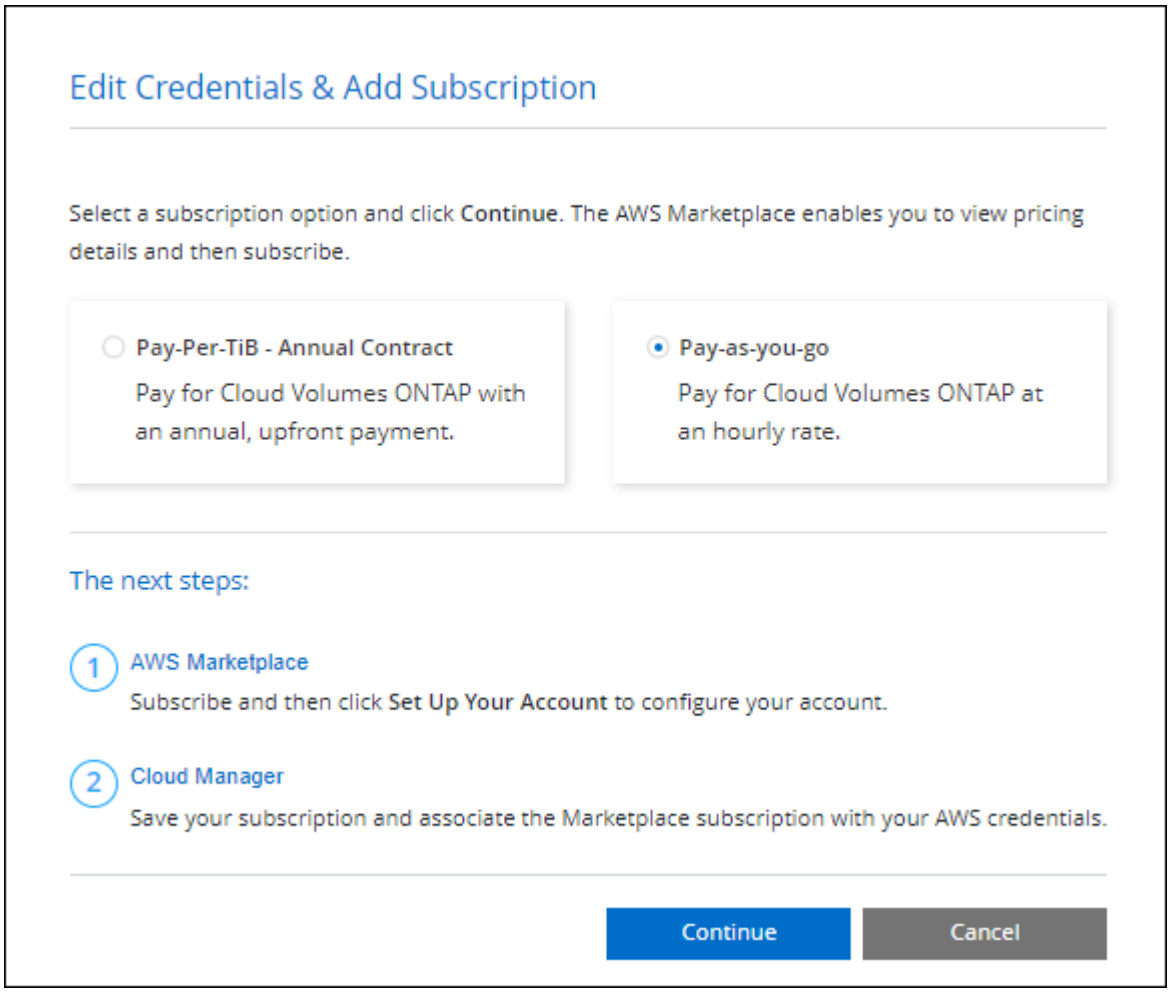
Seleziona l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con una capacità fornita fino a 500 GiB. "Scopri di più sull'offerta Freemium" .

Passi

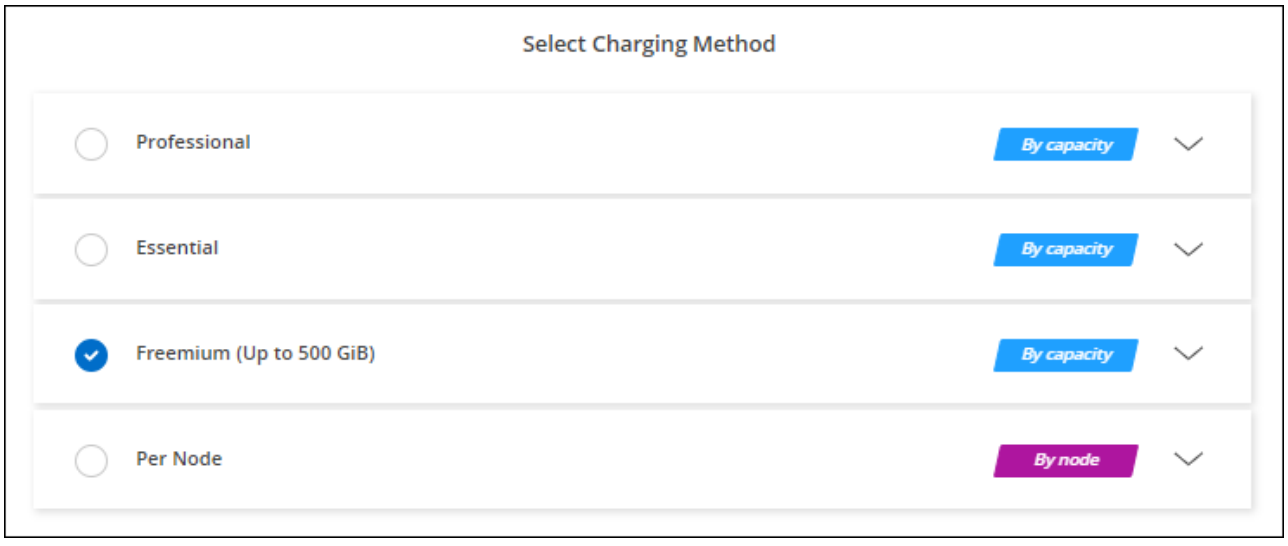
1. Dal menu di navigazione a sinistra della NetApp Console, selezionare **Storage > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.

    a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti all'offerta con pagamento in base al consumo in AWS Marketplace.

Non ti verrà addebitato alcun costo tramite l'abbonamento al marketplace a meno che tu non superi i 500 GiB di capacità fornita, momento in cui il sistema verrà automaticamente convertito in"Pacchetto essenziale" .



a. Dopo essere tornato alla Console, seleziona **Freemium** quando arrivi alla pagina dei metodi di addebito.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS" .

Licenza basata sulla capacità

Le licenze basate sulla capacità consentono di pagare Cloud Volumes ONTAP per TiB di capacità. Le licenze basate sulla capacità sono disponibili sotto forma di *pacchetto*: il pacchetto Essentials o il pacchetto Professional.

I pacchetti Essentials e Professional sono disponibili con i seguenti modelli di consumo o opzioni di acquisto:

- Una licenza (Bring Your Own License (BYOL)) acquistata da NetApp
- Un abbonamento orario con pagamento in base al consumo (PAYGO) da AWS Marketplace
- Un contratto annuale da AWS Marketplace

"Scopri di più sulle licenze basate sulla capacità" .

Le sezioni seguenti descrivono come iniziare a utilizzare ciascuno di questi modelli di consumo.

BYOL

Paga in anticipo acquistando una licenza (BYOL) da NetApp per distribuire i sistemi Cloud Volumes ONTAP in qualsiasi provider cloud.

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Passi

1. "Contatta NetApp Sales per ottenere una licenza"
2. "Aggiungi il tuo account del sito di supporto NetApp alla console"

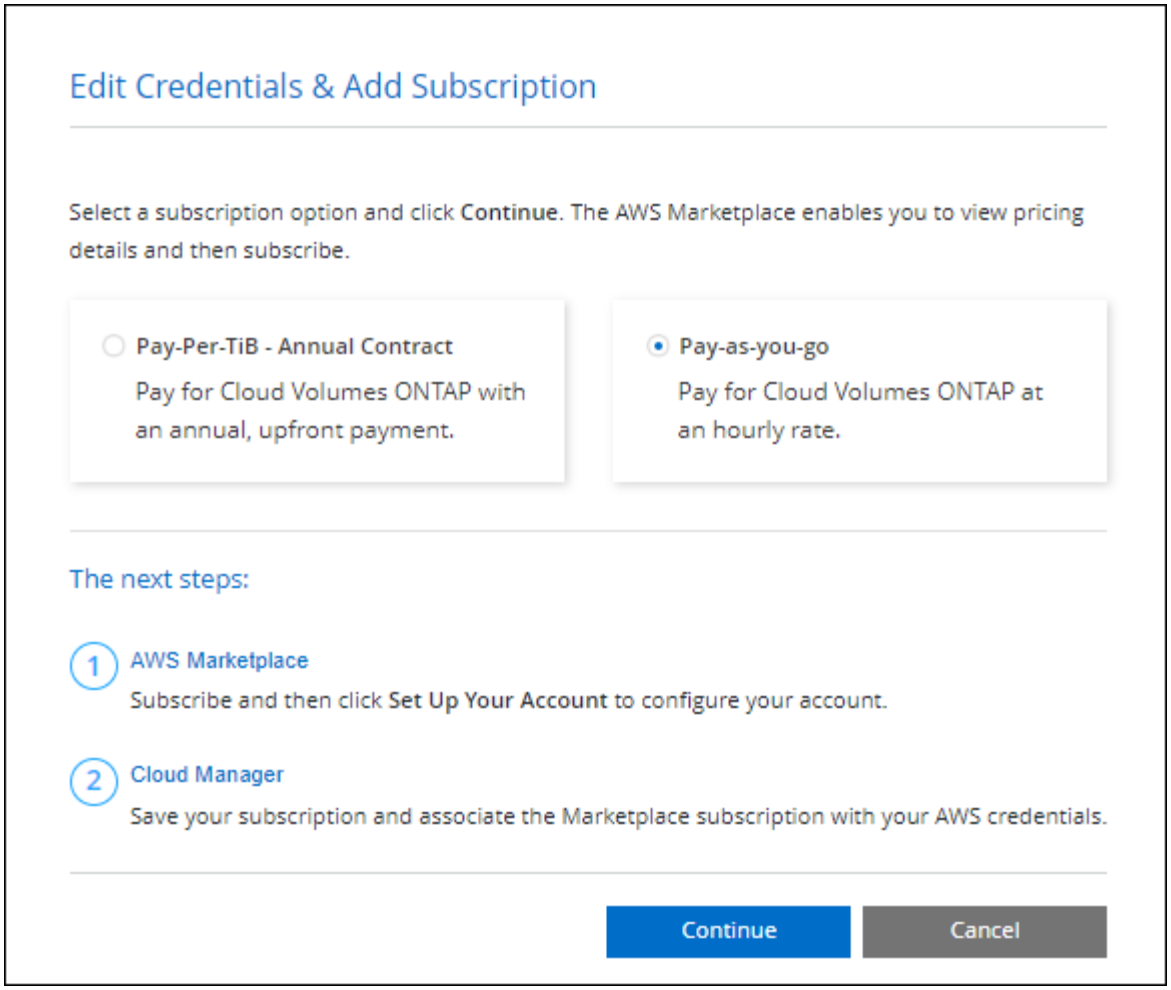
   La Console interroga automaticamente il servizio licenze di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. Se non ci sono errori, la Console aggiunge automaticamente le licenze alla Console.

   La licenza deve essere disponibile nella Console prima di poterla utilizzare con Cloud Volumes ONTAP. Se necessario, puoi"aggiungere manualmente la licenza alla Console" .

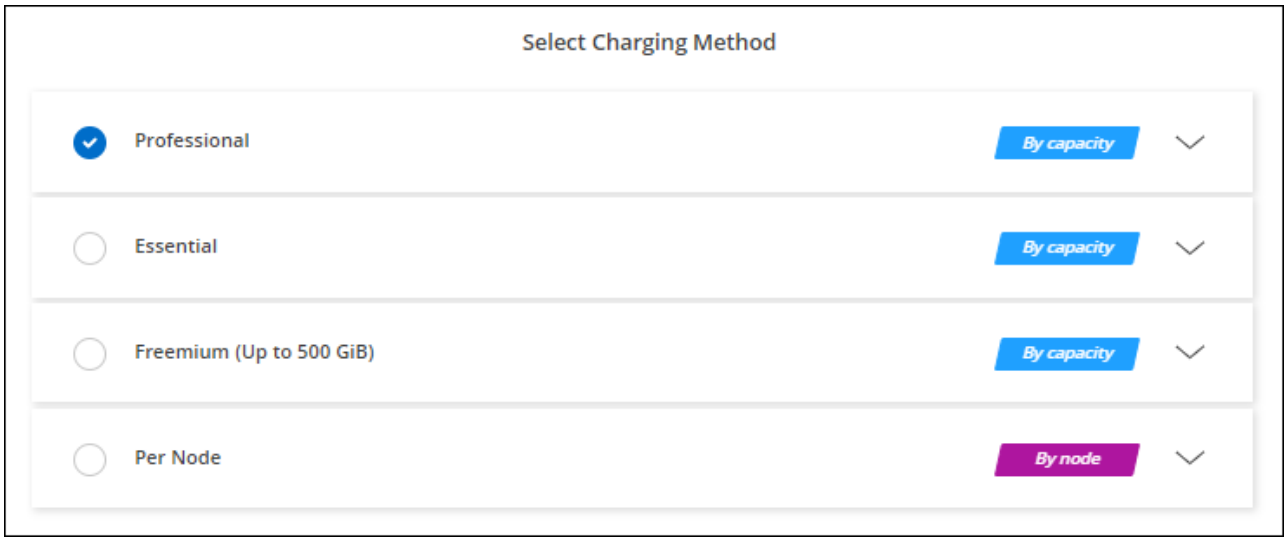
3. Nella pagina **Sistemi** della Console, fare clic su **Aggiungi sistema** e seguire i passaggi.

   a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti all'offerta con pagamento in base al consumo in AWS Marketplace.

      La licenza acquistata da NetApp viene sempre addebitata per prima, ma ti verrà addebitata la tariffa oraria del marketplace se superi la capacità della licenza o se scade il termine della licenza.



a. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS" .

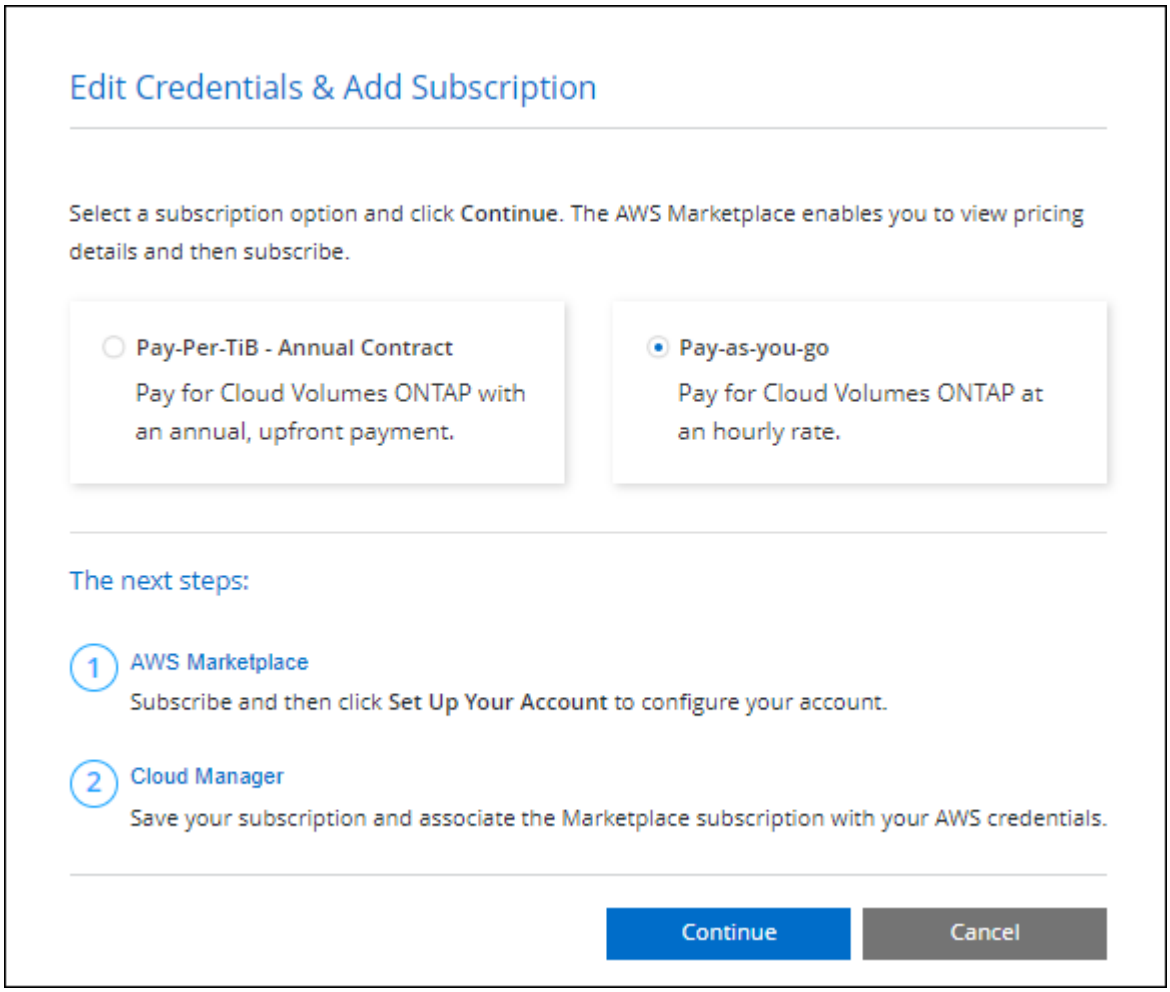
Abbonamento PAYGO

Paga a ore sottoscrivendo l'offerta dal marketplace del tuo provider cloud.

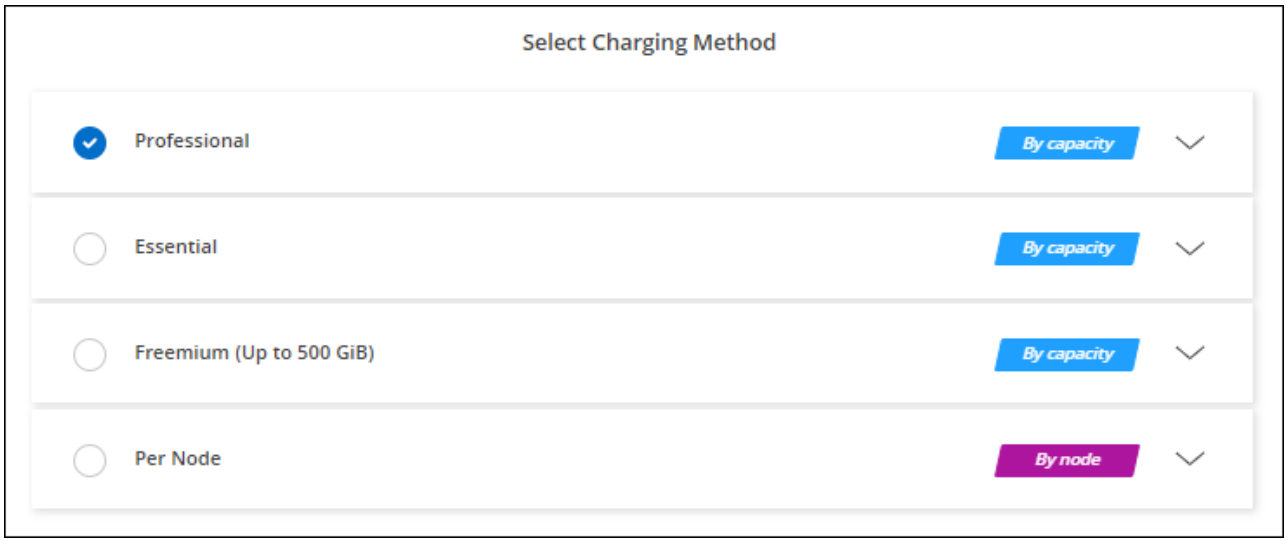
Quando si crea un sistema Cloud Volumes ONTAP , la Console richiede di sottoscrivere il contratto disponibile in AWS Marketplace. Tale abbonamento viene poi associato al sistema di addebito. È possibile utilizzare lo stesso abbonamento per altri sistemi Cloud Volumes ONTAP .

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti all'offerta con pagamento in base al consumo in AWS Marketplace



   b. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS" .

Puoi gestire gli abbonamenti AWS Marketplace associati ai tuoi account AWS dalla pagina Impostazioni > Credenziali. "Scopri come gestire i tuoi account e abbonamenti AWS"

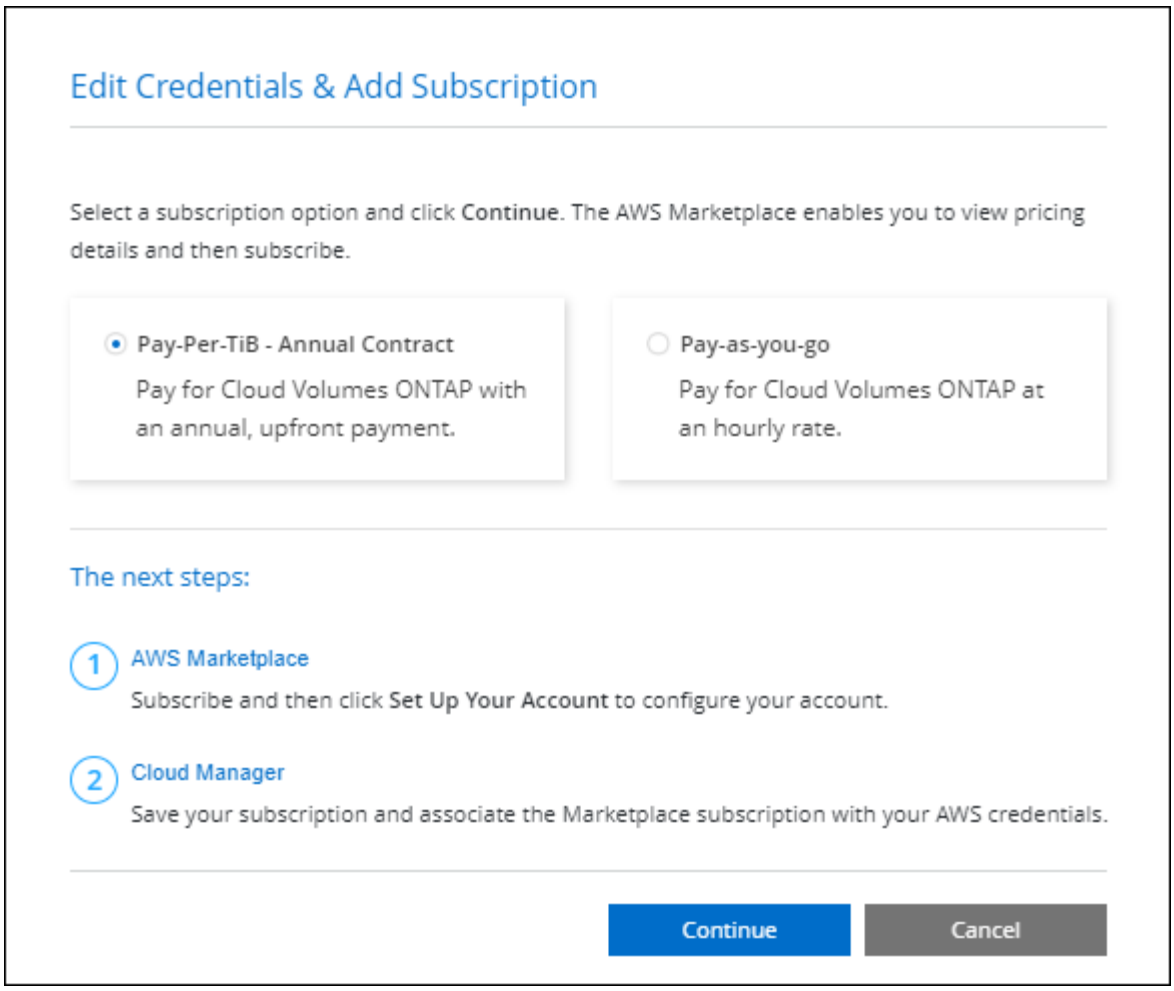
Contratto annuale

Paga annualmente acquistando un contratto annuale dal marketplace del tuo provider cloud.

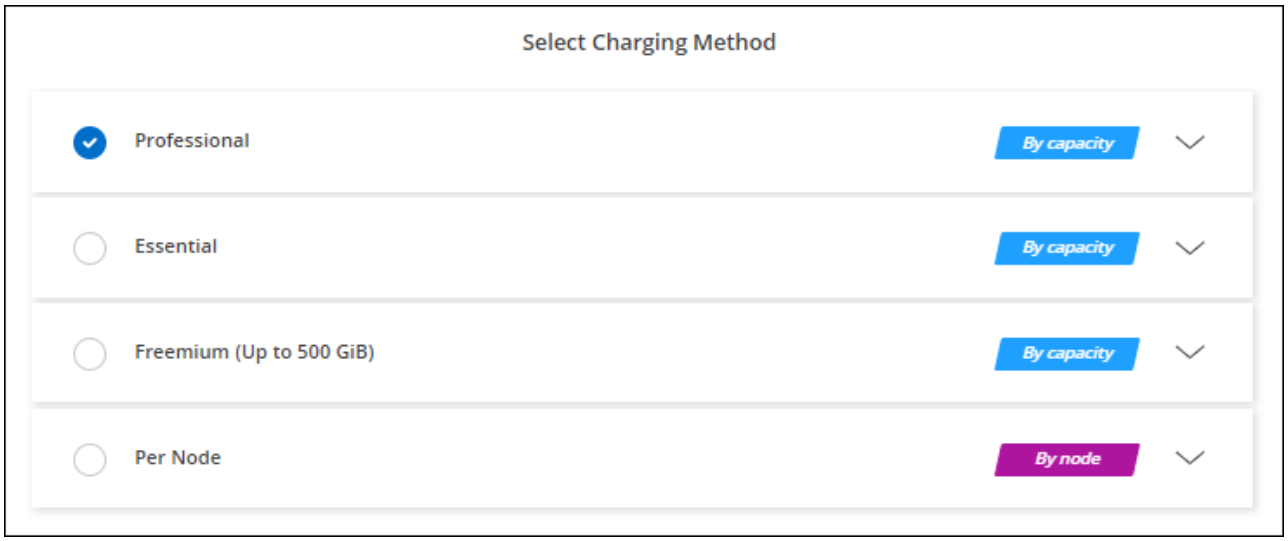
Analogamente a un abbonamento orario, la Console ti chiede di sottoscrivere il contratto annuale disponibile su AWS Marketplace.

Passi

1. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti al contratto annuale in AWS Marketplace.



b. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS" .

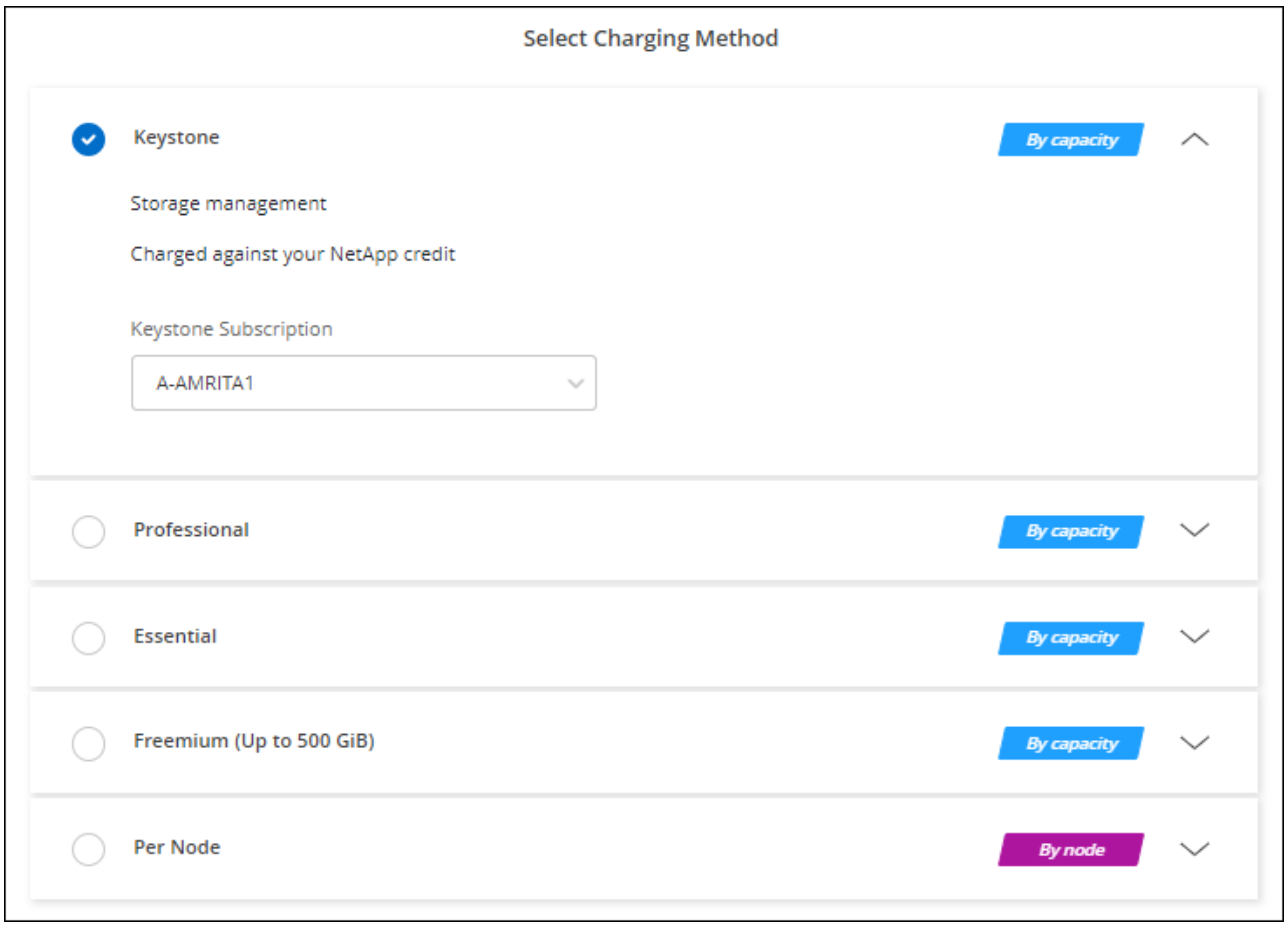
Abbonamento Keystone

Un abbonamento Keystone è un servizio basato su un abbonamento con pagamento in base alla crescita. "Scopri di più sugli abbonamenti NetApp Keystone" .

Passi

1. Se non hai ancora un abbonamento, "contattare NetApp"
2. Contatta NetApp per autorizzare il tuo account utente con uno o più abbonamenti Keystone .
3. Dopo che NetApp autorizza il tuo account,"collega i tuoi abbonamenti per utilizzarli con Cloud Volumes ONTAP" .
4. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.

    a. Quando ti viene richiesto di scegliere un metodo di addebito, seleziona il metodo di addebito Keystone Subscription.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS" .

Licenza basata su nodi

Una licenza basata su nodi è la licenza di precedente generazione per Cloud Volumes ONTAP. Una licenza basata su nodi può essere acquistata da NetApp (BYOL) ed è disponibile per i rinnovi di licenza solo in casi specifici. Per informazioni, fare riferimento a:

- "Fine della disponibilità delle licenze basate su nodi"

- "Fine della disponibilità delle licenze basate sui nodi"
- "Convertire una licenza basata su nodi in una licenza basata sulla capacità"

Distribuisci Cloud Volumes ONTAP in AWS utilizzando la distribuzione rapida

È possibile distribuire Cloud Volumes ONTAP in AWS utilizzando un metodo di distribuzione rapido sia per configurazioni a nodo singolo che ad alta disponibilità (HA). Questo processo semplificato riduce i passaggi di distribuzione rispetto al metodo avanzato. Offre inoltre maggiore chiarezza nel flusso di lavoro impostando automaticamente i valori predefiniti su una singola pagina e riducendo al minimo la navigazione.

Prima di iniziare

Per aggiungere un sistema Cloud Volumes ONTAP in AWS dalla NetApp Console, è necessario quanto segue.

- Un agente Console attivo e funzionante.
  - Dovresti avere un "Agente console associato al tuo progetto o spazio di lavoro" .
  - "Dovresti essere pronto a lasciare l'agente della console sempre in esecuzione" .
- Una comprensione della configurazione che si desidera utilizzare.

  Dovresti esserti preparato scegliendo una configurazione e ottenendo informazioni sulla rete AWS dal tuo amministratore. Per i dettagli, fare riferimento a"Pianificazione della configurazione Cloud Volumes ONTAP" .
- Una comprensione di ciò che è necessario per impostare la licenza per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze" .
- DNS e Active Directory per configurazioni CIFS.

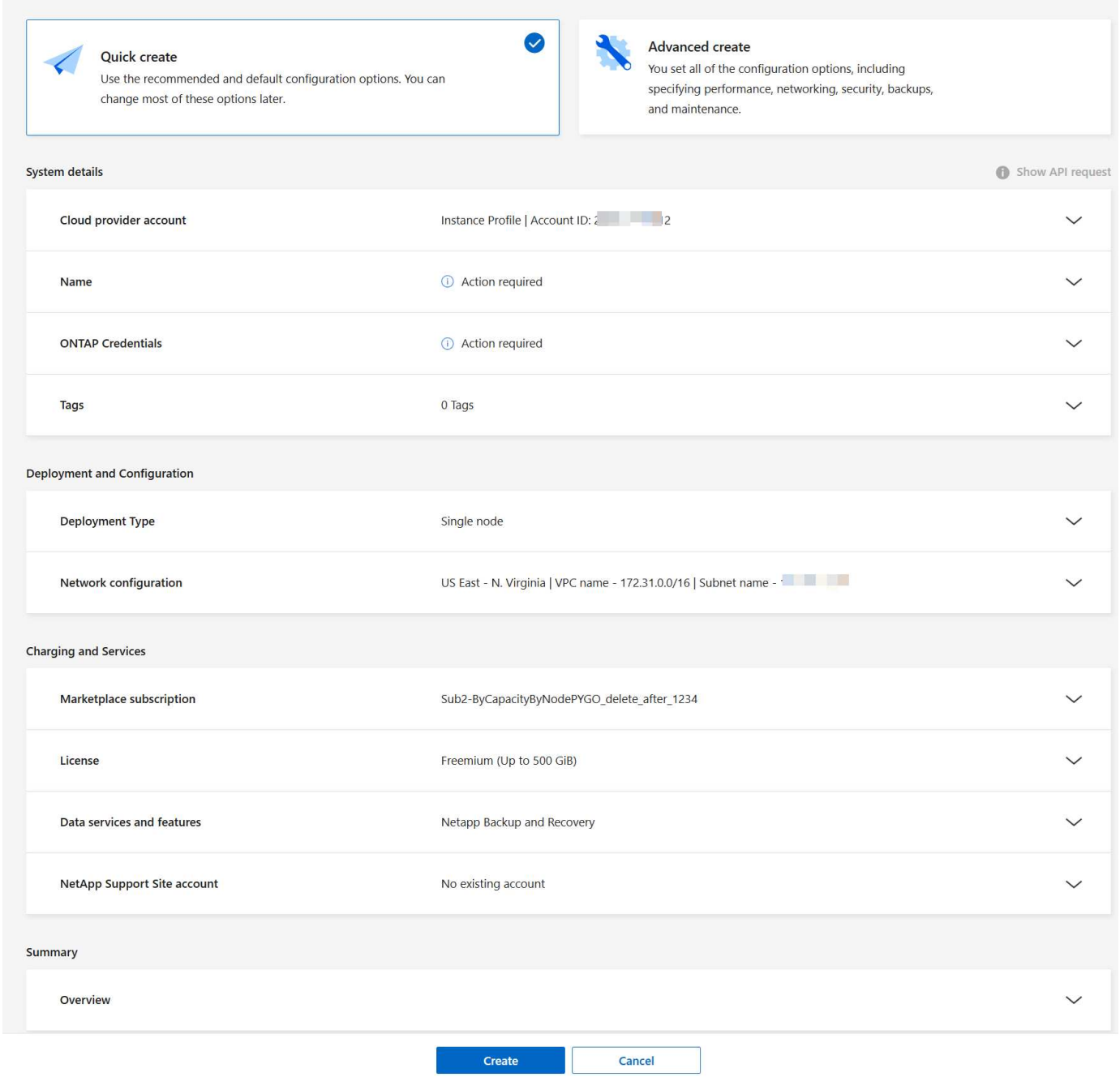
  Per i dettagli, fare riferimento a"Requisiti di rete per Cloud Volumes ONTAP in AWS" .

Informazioni su questo compito

Subito dopo aver creato il sistema Cloud Volumes ONTAP , la NetApp Console avvia un'istanza di prova nella VPC specificata per verificare la connettività. In caso di esito positivo, la Console termina immediatamente l'istanza e quindi avvia la distribuzione del sistema. Se la console non riesce a verificare la connettività, la creazione del sistema fallisce. L'istanza di prova è una `t2.nano` (per la locazione VPC predefinita) o un `m3.medium` (per tenancy VPC dedicata).

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina Canvas, clicca su **Aggiungi sistema** e segui le istruzioni.
3. Selezionare **Amazon Web Services** > * Cloud Volumes ONTAP* > **Aggiungi nuovo**. L'opzione **Creazione rapida** è selezionata per impostazione predefinita.



dettagli del sistema

1. **Account del provider cloud**: i dettagli dell'account vengono compilati automaticamente in base all'agente della console selezionato. Se hai più account, seleziona quello che desideri utilizzare. Se un agente della console non è disponibile, ti verrà richiesto di "creare un agente Console" .
2. **Nome**: Nome del sistema. La console utilizza il nome del sistema (cluster) per denominare il sistema Cloud Volumes ONTAP e l'istanza Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.
3. * Credenziali ONTAP * Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. È possibile mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.
4. **Tag** I tag AWS sono metadati per le tue risorse AWS. La console aggiunge i tag all'istanza Cloud Volumes ONTAP e a ciascuna risorsa AWS associata all'istanza. È possibile aggiungere fino a 15 tag dall'interfaccia

utente durante la creazione di un sistema Cloud Volumes ONTAP , per poi aggiungerne altri dopo la creazione. Tieni presente che l'API non ti limita a quattro tag quando crei un sistema. Per informazioni sui tag, fare riferimento a "Documentazione AWS: etichettatura delle risorse Amazon EC2" .

Distribuzione e configurazione

1. **Tipo di distribuzione**: seleziona il tipo di distribuzione che desideri utilizzare: nodo singolo, alta disponibilità (HA) in una singola zona di disponibilità (AZ) o HA in più AZ.
2. **Configurazione di rete**: inserisci le informazioni di rete che hai registrato nel "Foglio di lavoro AWS" .
   a. **Regione AWS**: per impostazione predefinita, viene selezionata la regione dell'account cloud associato che dispone di VPC con risorse di subnet.
   b. **VPC**: immettere una VPC per la regione AWS con una subnet. Se non sono presenti subnet, viene selezionato il valore predefinito per la VPC.
   c. **Sottorete**: è possibile selezionare una sottorete per la VPC solo per una distribuzione a nodo singolo o una distribuzione HA in una singola AZ.

Alta disponibilità

Se hai selezionato la configurazione HA, inserisci le seguenti informazioni:

HA in AZ singola

1. **Accesso mediatore**: specificare le informazioni di accesso del mediatore. Il mediatore è un'istanza separata che monitora lo stato di salute della coppia HA e fornisce il quorum in caso di errore. Fornire il nome della coppia di chiavi per consentire all'istanza del mediatore di connettersi al servizio AWS EC2 e selezionare il metodo di connessione.

HA in più AZ

1. **Zone di disponibilità e mediatore**: seleziona le zone di disponibilità (AZ) per ciascun nodo e il mediatore e le subnet corrispondenti in cui desideri distribuire la coppia Cloud Volumes ONTAP HA.
2. **IP mobili**: se si scelgono più AZ, specificare gli indirizzi IP mobili per i servizi NFS e CIFS e per la gestione di cluster e SVM. Gli indirizzi IP devono essere esterni al blocco CIDR per tutte le VPC nella regione. Per ulteriori dettagli, fare riferimento a"Requisiti di rete AWS per Cloud Volumes ONTAP HA in più AZ" .
3. **Accesso mediatore**: specificare le informazioni di accesso del mediatore. Il mediatore è un'istanza separata che monitora lo stato di salute della coppia HA e fornisce il quorum in caso di errore. Fornire il nome della coppia di chiavi per consentire all'istanza del mediatore di connettersi al servizio AWS EC2 e selezionare il metodo di connessione.
4. **Tabelle di routing**: se hai scelto più AZ, seleziona le tabelle di routing che includono i percorsi verso gli indirizzi IP mobili. Se si dispone di più di una tabella di routing, è importante selezionare le tabelle di routing corrette. In caso contrario, alcuni client potrebbero non avere accesso alla coppia Cloud Volumes ONTAP HA. Per ulteriori informazioni sulle tabelle di routing, fare riferimento a "Documentazione AWS: tabelle di routing" .

Ricarica e servizi

1. **Abbonamento Marketplace**: seleziona l'abbonamento AWS Marketplace che desideri utilizzare con questo sistema Cloud Volumes ONTAP .
2. **Licenza**: seleziona il tipo di licenza che desideri utilizzare con questo sistema Cloud Volumes ONTAP . Puoi scegliere tra le licenze Professional, Essential e Premium. Per informazioni sulle diverse licenze, fare riferimento a"Scopri di più sulle licenze Cloud Volumes ONTAP" .

3. **Servizi e funzionalità dati**: mantieni abilitati i servizi o disabilita quelli che non desideri utilizzare con Cloud Volumes ONTAP.
    - "Scopri di più sulla classificazione NetApp"
    - "Scopri di più su NetApp Backup and Recovery"
    - "Scopri di più sullo storage WORM su Cloud Volumes ONTAP"

      Se si desidera utilizzare WORM e il tiering dei dati, è necessario disabilitare Backup e ripristino e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

    - * Account del sito di supporto NetApp *: se disponi di più account, seleziona quello che desideri utilizzare.

Riepilogo

Controlla o modifica i dettagli inseriti, quindi fai clic su **Crea**.

Una volta completato il processo di distribuzione, non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale cloud AWS, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdite di dati.

Link correlati

- "Pianificazione della configurazione Cloud Volumes ONTAP"
- "Distribuisci Cloud Volumes ONTAP in AWS utilizzando la distribuzione avanzata"

Avvia Cloud Volumes ONTAP in AWS

È possibile avviare Cloud Volumes ONTAP in una configurazione a sistema singolo o come coppia HA in AWS. Questo metodo fornisce un'esperienza di distribuzione avanzata che offre più opzioni di configurazione e flessibilità rispetto al metodo di distribuzione rapida.

Prima di iniziare

Prima di iniziare, ti occorre quanto segue.

- Un agente Console attivo e funzionante.
    - Dovresti avere un "Agente console associato al tuo sistema" .
    - "Dovresti essere pronto a lasciare l'agente della console sempre in esecuzione" .
- Una comprensione della configurazione che si desidera utilizzare.

  Dovresti esserti preparato scegliendo una configurazione e ottenendo informazioni sulla rete AWS dal tuo amministratore. Per i dettagli, fare riferimento a"Pianificazione della configurazione Cloud Volumes ONTAP" .

- Una comprensione di ciò che è necessario per impostare la licenza per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze" .

- DNS e Active Directory per configurazioni CIFS.

Per i dettagli, fare riferimento a"Requisiti di rete per Cloud Volumes ONTAP in AWS" .

Avvia un sistema Cloud Volumes ONTAP a nodo singolo in AWS

Se si desidera avviare Cloud Volumes ONTAP in AWS, è necessario creare un nuovo sistema nella NetApp Console.

Informazioni su questo compito

Subito dopo aver creato il sistema, la Console avvia un'istanza di prova nella VPC specificata per verificare la connettività. In caso di esito positivo, la Console termina immediatamente l'istanza e avvia la distribuzione del sistema Cloud Volumes ONTAP . Se la connettività non può essere verificata, la creazione del sistema fallisce. L'istanza di prova è una `t2.nano` (per la locazione VPC predefinita) o `m3.medium` (per tenancy VPC dedicata).

Passi

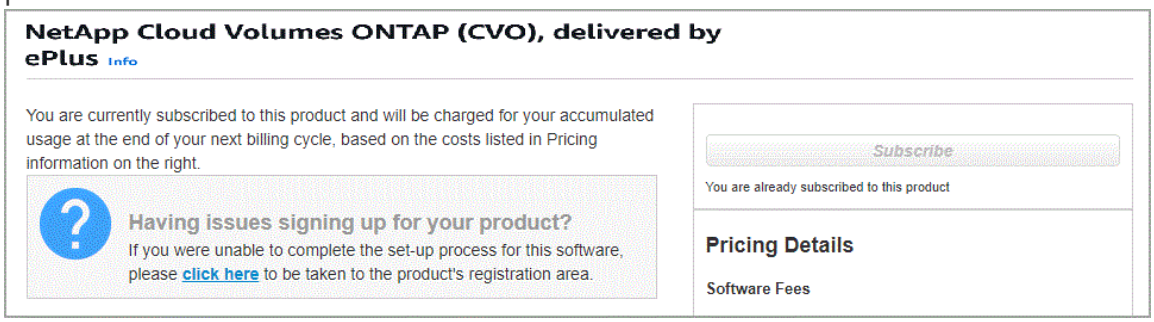
1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire le istruzioni.
3. Selezionare **Amazon Web Services** e * Cloud Volumes ONTAP Single Node*.
4. Seleziona **Creazione avanzata**. Poiché per impostazione predefinita è selezionata la modalità **Creazione rapida**, potrebbe essere visualizzato un messaggio per i valori predefiniti. Fare clic su **Continua**.
5. Se richiesto, "creare un agente Console" .
6. **Dettagli e credenziali**: facoltativamente, modifica le credenziali e l'abbonamento AWS, inserisci un nome di sistema, aggiungi tag se necessario e quindi inserisci una password.

   Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia l'istanza Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.
Aggiungi tag	I tag AWS sono metadati per le tue risorse AWS. La console aggiunge i tag all'istanza Cloud Volumes ONTAP e a ciascuna risorsa AWS associata all'istanza. Quando si crea un sistema, è possibile aggiungere fino a quattro tag dall'interfaccia utente, per poi aggiungerne altri dopo la creazione. Tieni presente che l'API non ti limita a quattro tag quando crei un sistema. Per informazioni sui tag, fare riferimento a "Documentazione AWS: etichettatura delle risorse Amazon EC2" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.

Campo	Descrizione
Modifica credenziali	Seleziona le credenziali AWS associate all'account in cui desideri distribuire questo sistema. È anche possibile associare l'abbonamento AWS Marketplace da utilizzare con questo sistema Cloud Volumes ONTAP . Fai clic su **Aggiungi abbonamento** per associare le credenziali selezionate a un nuovo abbonamento al marketplace AWS. L'abbonamento può essere stipulato con un contratto annuale o con il pagamento di Cloud Volumes ONTAP a tariffa oraria. "Scopri come aggiungere ulteriori credenziali AWS alla NetApp Console" .

Se più utenti IAM lavorano nello stesso account AWS, ogni utente deve abbonarsi. Dopo che il primo utente si è iscritto, AWS Marketplace informa gli utenti successivi che sono già iscritti, come mostrato nell'immagine sottostante. Finché è attivo un abbonamento per l'account AWS, ogni utente IAM deve associarsi a tale abbonamento. Se vedi il messaggio mostrato di seguito, clicca sul link **clicca qui** per andare al sito web della Console e completare la
procedura.



7. **Servizi**: mantieni abilitati i servizi o disabilita i singoli servizi che non desideri utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla NetApp Data Classification"
   - "Scopri di più su NetApp Backup and Recovery"

   Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

8. **Posizione e connettività**: inserisci le informazioni di rete che hai registrato nel "Foglio di lavoro AWS" .

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
VPC	Se disponi di un AWS Outpost, puoi distribuire un sistema Cloud Volumes ONTAP a nodo singolo in quell'Outpost selezionando l'Outpost VPC. L'esperienza è la stessa di qualsiasi altra VPC residente in AWS.

Campo	Descrizione
Gruppo di sicurezza generato	Se lasci che sia la Console a generare il gruppo di sicurezza per te, devi scegliere come consentire il traffico: • Se si sceglie **Solo VPC selezionata**, l'origine del traffico in entrata è l'intervallo di subnet della VPC selezionata e l'intervallo di subnet della VPC in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le VPC**, la sorgente del traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizza il gruppo di sicurezza esistente	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. "Scopri le regole del firewall per Cloud Volumes ONTAP" .

9. **Crittografia dei dati**: scegli nessuna crittografia dei dati o la crittografia gestita da AWS.

   Per la crittografia gestita da AWS, puoi scegliere una Customer Master Key (CMK) diversa dal tuo account o da un altro account AWS.

   Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP .

   "Scopri come configurare AWS KMS per Cloud Volumes ONTAP" .

   "Scopri di più sulle tecnologie di crittografia supportate" .

10. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp .
    - "Scopri le opzioni di licenza per Cloud Volumes ONTAP" .
    - "Scopri come impostare le licenze" .
11. * Configurazione Cloud Volumes ONTAP * (solo contratto annuale AWS Marketplace): rivedere la configurazione predefinita e fare clic su **Continua** oppure fare clic su **Modifica configurazione** per selezionare la propria configurazione.

    Se si mantiene la configurazione predefinita, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

12. **Pacchetti preconfigurati**: seleziona uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fai clic su **Modifica configurazione** per selezionare la tua configurazione.

    Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

13. **Ruolo IAM**: è meglio mantenere l'opzione predefinita per consentire alla Console di creare il ruolo per te.

    Se preferisci utilizzare la tua polizza, questa deve soddisfare"requisiti di policy per i nodi Cloud Volumes ONTAP" .

14. **Licenze**: modifica la versione Cloud Volumes ONTAP in base alle tue esigenze e seleziona un tipo di istanza e la locazione dell'istanza.

Se per la versione selezionata è disponibile una versione Release Candidate, General Availability o patch più recente, la Console aggiorna il sistema a tale versione durante la creazione del sistema. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.13.1 e se è disponibile la versione 9.13.1 P4. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.13 alla 9.14.

15. **Risorse di archiviazione sottostanti**: scegli un tipo di disco, configura l'archiviazione sottostante e scegli se mantenere abilitata la suddivisione in livelli dei dati.

    Notare quanto segue:

    - Il tipo di disco è per il volume iniziale (e aggregato). È possibile scegliere un tipo di disco diverso per i volumi successivi (e aggregati).
    - Se si sceglie un disco gp3 o io1, la Console utilizza la funzionalità Elastic Volumes di AWS per aumentare automaticamente la capacità del disco di archiviazione sottostante in base alle esigenze. È possibile scegliere la capacità iniziale in base alle proprie esigenze di archiviazione e modificarla dopo l'implementazione Cloud Volumes ONTAP . "Scopri di più sul supporto per Elastic Volumes in AWS" .
    - Se si sceglie un disco gp2 o st1, è possibile selezionare una dimensione del disco per tutti i dischi nell'aggregato iniziale e per tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.
    - Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
    - Se si disabilita la suddivisione in livelli dei dati, è possibile abilitarla sugli aggregati successivi.

      "Scopri come funziona il data tiering" .

16. **Velocità di scrittura e WORM**:

    a. Se lo desideri, seleziona la velocità di scrittura **Normale** o **Alta**.

       "Scopri di più sulla velocità di scrittura" .

    b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

       WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

    "Scopri di più sullo storage WORM" .

    a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.

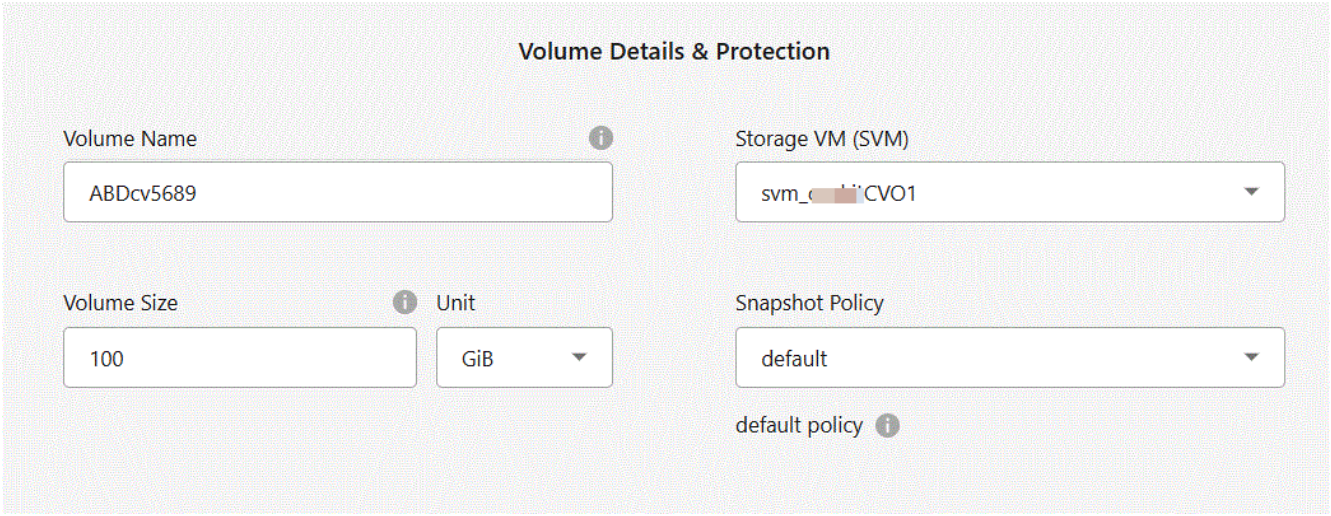
17. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

    "Scopri i protocolli e le versioni client supportati" .

    Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



18. **Configurazione CIFS**: se hai scelto il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Se si configura AWS Managed Microsoft AD come server AD per Cloud Volumes ONTAP, è necessario immettere **OU=Computers,OU=corp** in questo campo.
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

19. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Comprensione dei profili di utilizzo del volume" ,"Panoramica della suddivisione in livelli dei dati" , E "KB: Quali funzionalità di Inline Storage Efficiency sono supportate da CVO?"

20. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fare clic su **Ulteriori informazioni** per visualizzare i dettagli sul supporto e sulle risorse AWS che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console avvia l'istanza Cloud Volumes ONTAP . È possibile monitorare i progressi nella pagina **Audit**.

In caso di problemi durante l'avvio dell'istanza di Cloud Volumes ONTAP , rivedere il messaggio di errore. È anche possibile selezionare il sistema e fare clic su **Ricrea ambiente**.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

Una volta completato il processo di distribuzione, non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale cloud AWS, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdite di dati.

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Avvia una coppia Cloud Volumes ONTAP HA in AWS

Se si desidera avviare una coppia Cloud Volumes ONTAP HA in AWS, è necessario creare un sistema HA nella Console.

Limitazione

Al momento, le coppie HA non sono supportate con AWS Outposts.

Informazioni su questo compito

Subito dopo aver creato il sistema Cloud Volumes ONTAP , la Console avvia un'istanza di prova nella VPC specificata per verificare la connettività. In caso di esito positivo, la Console termina immediatamente l'istanza e avvia la distribuzione del sistema Cloud Volumes ONTAP . Se la connettività non può essere verificata, la creazione del sistema fallisce. L'istanza di prova è una `t2.nano` (per la locazione VPC predefinita) o `m3.medium` (per tenancy VPC dedicata).

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire le istruzioni.
3. Selezionare **Amazon Web Services** e * Cloud Volumes ONTAP HA*.

   Sono disponibili alcune zone locali AWS.

   Prima di poter utilizzare le zone locali AWS, è necessario abilitarle e creare una subnet nella zona locale nel proprio account AWS. Segui i passaggi **Accedi a una zona locale AWS** ed **Estendi la tua Amazon VPC alla zona locale** nella"Tutorial AWS "Inizia a distribuire applicazioni a bassa latenza con le zone locali AWS"" .

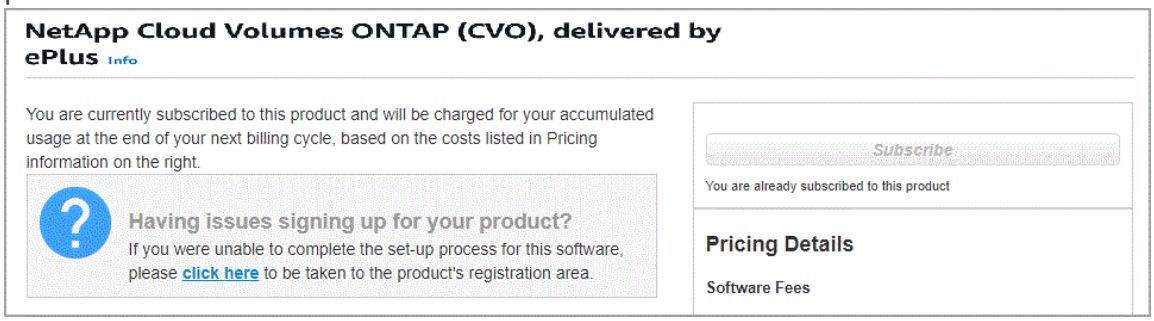
   Se si esegue l'agente Console 3.9.36 o versione precedente, è necessario aggiungere `DescribeAvailabilityZones` autorizzazione al ruolo AWS nella console AWS EC2.

4. **Dettagli e credenziali**: facoltativamente, modifica le credenziali e l'abbonamento AWS, inserisci un nome di sistema, aggiungi tag se necessario e quindi inserisci una password.

   Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia l'istanza Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.
Aggiungi tag	I tag AWS sono metadati per le tue risorse AWS. La console aggiunge i tag all'istanza Cloud Volumes ONTAP e a ciascuna risorsa AWS associata all'istanza. Quando si crea un sistema, è possibile aggiungere fino a quattro tag dall'interfaccia utente, per poi aggiungerne altri dopo la creazione. Tieni presente che l'API non ti limita a quattro tag quando crei un sistema. Per informazioni sui tag, fare riferimento a "Documentazione AWS: etichettatura delle risorse Amazon EC2" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.
Modifica credenziali	Seleziona le credenziali AWS e l'abbonamento al marketplace da utilizzare con questo sistema Cloud Volumes ONTAP . Fai clic su **Aggiungi abbonamento** per associare le credenziali selezionate a un nuovo abbonamento al marketplace AWS. L'abbonamento può essere stipulato con un contratto annuale o con il pagamento di Cloud Volumes ONTAP a tariffa oraria. Se hai acquistato una licenza direttamente da NetApp (Bring Your Own License (BYOL)), non è necessario un abbonamento AWS. NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" . "Scopri come aggiungere ulteriori credenziali AWS alla Console" .

Se più utenti IAM lavorano nello stesso account AWS, ogni utente deve abbonarsi. Dopo che il primo utente si è iscritto, AWS Marketplace informa gli utenti successivi che sono già iscritti, come mostrato nell'immagine sottostante. Finché è attivo un abbonamento per l'account AWS, ogni utente IAM deve associarsi a tale abbonamento. Se vedi il messaggio mostrato di seguito, clicca sul link **clicca qui** per andare al sito web della Console e completare la
procedura.



5. **Servizi**: mantieni abilitati i servizi o disabilita i singoli servizi che non desideri utilizzare con questo sistema Cloud Volumes ONTAP .
   - "Scopri di più sulla NetApp Data Classification"
   - "Scopri di più su Backup e Ripristino"

Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

6. **Modelli di distribuzione HA**: scegli una configurazione HA.

   Per una panoramica dei modelli di distribuzione, fare riferimento a"Cloud Volumes ONTAP HA per AWS" .

7. **Posizione e connettività** (singola zona di disponibilità (AZ)) o **Regione e VPC** (più AZ): inserisci le informazioni di rete registrate nel foglio di lavoro AWS.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Gruppo di sicurezza generato	Se lasci che sia la Console a generare il gruppo di sicurezza per te, devi scegliere come consentire il traffico: • Se si sceglie **Solo VPC selezionata**, l'origine del traffico in entrata è l'intervallo di subnet della VPC selezionata e l'intervallo di subnet della VPC in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le VPC**, la sorgente del traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizza il gruppo di sicurezza esistente	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. "Scopri le regole del firewall per Cloud Volumes ONTAP" .

8. **Connettività e autenticazione SSH**: scegliere i metodi di connessione per la coppia HA e il mediatore.
9. **IP mobili**: se hai scelto più AZ, specifica gli indirizzi IP mobili.

   Gli indirizzi IP devono essere esterni al blocco CIDR per tutte le VPC nella regione. Per ulteriori dettagli, fare riferimento a"Requisiti di rete AWS per Cloud Volumes ONTAP HA in più AZ" .

10. **Tabelle di routing**: se hai scelto più AZ, seleziona le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili.

    Se si dispone di più di una tabella di routing, è molto importante selezionare le tabelle di routing corrette. In caso contrario, alcuni client potrebbero non avere accesso alla coppia Cloud Volumes ONTAP HA. Per ulteriori informazioni sulle tabelle di routing, fare riferimento a "Documentazione AWS: tabelle di routing" .

11. **Crittografia dei dati**: scegli nessuna crittografia dei dati o la crittografia gestita da AWS.

    Per la crittografia gestita da AWS, puoi scegliere una Customer Master Key (CMK) diversa dal tuo account o da un altro account AWS.

    Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP .

    "Scopri come configurare AWS KMS per Cloud Volumes ONTAP" .

    "Scopri di più sulle tecnologie di crittografia supportate" .

12. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp .
    - "Scopri le opzioni di licenza per Cloud Volumes ONTAP" .
    - "Scopri come impostare le licenze" .
13. * Configurazione Cloud Volumes ONTAP * (solo contratto annuale AWS Marketplace): rivedere la configurazione predefinita e fare clic su **Continua** oppure fare clic su **Modifica configurazione** per selezionare la propria configurazione.

    Se si mantiene la configurazione predefinita, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

14. **Pacchetti preconfigurati** (solo orari o BYOL): seleziona uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fai clic su **Modifica configurazione** per selezionare la tua configurazione.

    Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

15. **Ruolo IAM**: è meglio mantenere l'opzione predefinita per consentire alla Console di creare il ruolo per te.

    Se preferisci utilizzare la tua polizza, questa deve soddisfare"requisiti di policy per i nodi Cloud Volumes ONTAP e il mediatore HA" .

16. **Licenze**: modifica la versione Cloud Volumes ONTAP in base alle tue esigenze e seleziona un tipo di istanza e la locazione dell'istanza.

    > Se per la versione selezionata è disponibile una versione Release Candidate, General Availability o patch più recente, la Console aggiorna il sistema a tale versione durante la creazione del sistema. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.13.1 e se è disponibile la versione 9.13.1 P4. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.13 alla 9.14.

17. **Risorse di archiviazione sottostanti**: scegli un tipo di disco, configura l'archiviazione sottostante e scegli se mantenere abilitata la suddivisione in livelli dei dati.

    Notare quanto segue:

    - Il tipo di disco è per il volume iniziale (e aggregato). È possibile scegliere un tipo di disco diverso per i volumi successivi (e aggregati).
    - Se si sceglie un disco gp3 o io1, la Console utilizza la funzionalità Elastic Volumes di AWS per aumentare automaticamente la capacità del disco di archiviazione sottostante in base alle esigenze. È possibile scegliere la capacità iniziale in base alle proprie esigenze di archiviazione e modificarla dopo l'implementazione Cloud Volumes ONTAP . "Scopri di più sul supporto per Elastic Volumes in AWS" .
    - Se si sceglie un disco gp2 o st1, è possibile selezionare una dimensione del disco per tutti i dischi nell'aggregato iniziale e per tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.
    - Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
    - Se si disabilita la suddivisione in livelli dei dati, è possibile abilitarla sugli aggregati successivi.

      "Scopri come funziona il data tiering" .

18. **Velocità di scrittura e WORM**:

    a. Se lo desideri, seleziona la velocità di scrittura **Normale** o **Alta**.

       "Scopri di più sulla velocità di scrittura" .

    b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

       WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

    "Scopri di più sullo storage WORM" .

    a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.

19. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

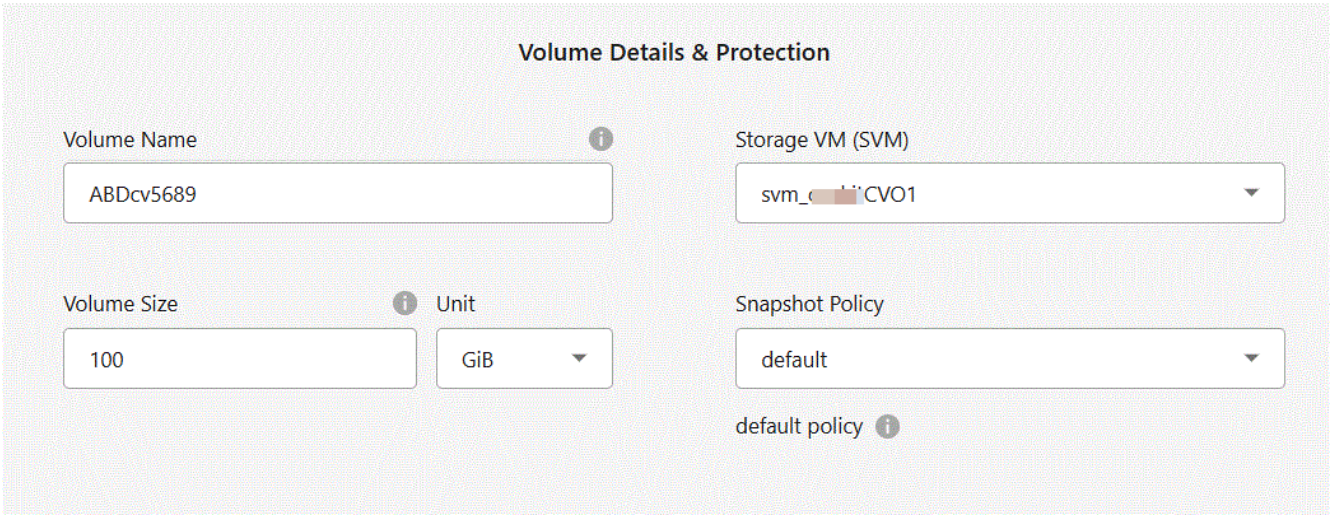
    "Scopri i protocolli e le versioni client supportati" .

    Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.

Campo	Descrizione
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



20. **Configurazione CIFS**: se hai selezionato il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Se si configura AWS Managed Microsoft AD come server AD per Cloud Volumes ONTAP, è necessario immettere **OU=Computers,OU=corp** in questo campo.

Campo	Descrizione
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

21. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Scegli un profilo di utilizzo del volume" E"Panoramica della suddivisione in livelli dei dati" .

22. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fare clic su **Ulteriori informazioni** per visualizzare i dettagli sul supporto e sulle risorse AWS che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console avvia la coppia Cloud Volumes ONTAP HA. È possibile monitorare i progressi nella pagina **Audit**.

Se si verificano problemi durante l'avvio della coppia HA, rivedere il messaggio di errore. È anche possibile selezionare il sistema e fare clic su Ricrea ambiente.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

> Una volta completato il processo di distribuzione, non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale cloud AWS, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdite di dati.

Link correlati

- "Pianificazione della configurazione Cloud Volumes ONTAP"
- "Distribuisci Cloud Volumes ONTAP in AWS utilizzando la distribuzione rapida"

Distribuisci Cloud Volumes ONTAP in AWS Secret Cloud o AWS Top Secret Cloud

Simile a una regione AWS standard, puoi utilizzare la NetApp Console in"Cloud segreto AWS" e in"Cloud top secret di AWS" per distribuire Cloud Volumes ONTAP, che fornisce funzionalità di livello aziendale per il tuo storage cloud. AWS Secret Cloud e Top Secret Cloud sono regioni chiuse specifiche della US Intelligence Community; le istruzioni in questa pagina si applicano solo agli utenti delle regioni AWS Secret Cloud e Top Secret Cloud.

Prima di iniziare

Prima di iniziare, controlla le versioni supportate in AWS Secret Cloud e Top Secret Cloud e scopri di più sulla modalità privata nella Console.

- Esamina le seguenti versioni supportate in AWS Secret Cloud e Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2
  - Versione 3.9.32 dell'agente Console

    L'agente Console è necessario per distribuire e gestire Cloud Volumes ONTAP in AWS. Accederai alla Console tramite il software installato sull'istanza dell'agente Console. Il sito Web SaaS per la console non è supportato in AWS Secret Cloud e Top Secret Cloud.
- Scopri di più sulla modalità privata

  In AWS Secret Cloud e Top Secret Cloud, la console funziona in *modalità privata*. In modalità privata, non c'è connettività al livello SaaS dalla Console. È possibile accedere alla Console tramite un'applicazione locale basata sul Web in grado di accedere all'agente della Console.

  Per saperne di più sul funzionamento della modalità privata, fare riferimento a"la modalità di distribuzione privata nella Console" .

Passaggio 1: configura la tua rete

Configura la tua rete AWS in modo che Cloud Volumes ONTAP possa funzionare correttamente.

Passi

1. Selezionare la VPC e le subnet in cui si desidera avviare l'istanza dell'agente Console e le istanze Cloud Volumes ONTAP .
2. Assicurati che la tua VPC e le tue subnet supportino la connettività tra l'agente della console e Cloud Volumes ONTAP.
3. Configura un endpoint VPC per il servizio Amazon Simple Storage Service (Amazon S3).

   È necessario un endpoint VPC se si desidera suddividere i dati inattivi da Cloud Volumes ONTAP in un archivio di oggetti a basso costo.

Passaggio 2: impostare le autorizzazioni

Imposta policy e ruoli IAM che forniscono all'agente della console e a Cloud Volumes ONTAP le autorizzazioni necessarie per eseguire azioni in AWS Secret Cloud o Top Secret Cloud.

Sono necessari un criterio IAM e un ruolo IAM per ciascuno dei seguenti elementi:

- L’istanza dell’agente Console
- Istanze Cloud Volumes ONTAP
- Per le coppie HA, l’istanza del mediatore HA Cloud Volumes ONTAP (se si desidera distribuire coppie HA)

Passi

1. Vai alla console AWS IAM e fai clic su **Criteri**.
2. Creare una policy per l’istanza dell’agente Console.

> È possibile creare queste policy per supportare i bucket S3 nel proprio ambiente AWS. Durante la creazione successiva dei bucket, assicurarsi che i nomi dei bucket siano preceduti da `fabric-pool-` . Questo requisito si applica sia alle regioni AWS Secret Cloud che Top Secret Cloud.

Regioni segrete

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regioni top secret

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Creare una policy per Cloud Volumes ONTAP.

Regioni segrete

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regioni top secret

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Per le coppie HA, se si prevede di distribuire una coppia Cloud Volumes ONTAP HA, creare una policy per il mediatore HA.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Crea ruoli IAM con il tipo di ruolo Amazon EC2 e collega le policy create nei passaggi precedenti.

   Crea il ruolo:

   Analogamente ai criteri, dovresti avere un ruolo IAM per l'agente della console e uno per i nodi Cloud Volumes ONTAP . Per coppie HA: analogamente ai criteri, dovresti avere un ruolo IAM per l'agente della console, uno per i nodi Cloud Volumes ONTAP e uno per il mediatore HA (se desideri distribuire coppie HA).

   Seleziona il ruolo:

   Quando si avvia l'istanza dell'agente Console, è necessario selezionare il ruolo IAM dell'agente Console. È possibile selezionare i ruoli IAM per Cloud Volumes ONTAP quando si crea un sistema Cloud Volumes ONTAP dalla Console. Per le coppie HA, è possibile selezionare i ruoli IAM per Cloud Volumes ONTAP e il mediatore HA quando si crea un sistema Cloud Volumes ONTAP .

Passaggio 3: configurazione di AWS KMS

Se si desidera utilizzare la crittografia Amazon con Cloud Volumes ONTAP, assicurarsi che siano soddisfatti i requisiti per AWS Key Management Service (KMS).

Passi

1. Assicurati che nel tuo account o in un altro account AWS sia presente una Customer Master Key (CMK) attiva.

   La CMK può essere una CMK gestita da AWS o una CMK gestita dal cliente.

2. Se la CMK si trova in un account AWS diverso dall'account in cui si prevede di distribuire Cloud Volumes ONTAP, è necessario ottenere l'ARN di tale chiave.

   È necessario fornire l'ARN alla Console quando si crea il sistema Cloud Volumes ONTAP .

3. Aggiungere il ruolo IAM per l'istanza all'elenco degli utenti chiave per una CMK.

   Ciò fornisce alla Console le autorizzazioni per utilizzare CMK con Cloud Volumes ONTAP.

Passaggio 4: installare l'agente Console e configurare la Console

Prima di poter iniziare a utilizzare la Console per distribuire Cloud Volumes ONTAP in AWS, è necessario installare e configurare l'agente della Console. Consente alla Console di gestire risorse e processi all'interno del tuo ambiente cloud pubblico (incluso Cloud Volumes ONTAP).

Passi

1. Ottieni un certificato radice firmato da un'autorità di certificazione (CA) nel formato X.509 codificato Base-64 Privacy Enhanced Mail (PEM). Consulta le politiche e le procedure della tua organizzazione per ottenere il certificato.

   > Per le regioni AWS Secret Cloud, dovresti caricare il `NSS Root CA 2` certificato, e per Top Secret Cloud, il `Amazon Root CA 4` certificato. Assicurati di caricare solo questi certificati e non l'intera catena. Il file per la catena di certificati è di grandi dimensioni e il caricamento potrebbe non riuscire. Se disponi di ulteriori certificati, puoi caricarli in un secondo momento, come descritto nel passaggio successivo.

   È necessario caricare il certificato durante la procedura di configurazione. La console utilizza il certificato attendibile quando invia richieste ad AWS tramite HTTPS.

2. Avviare l'istanza dell'agente Console:
   a. Vai alla pagina AWS Intelligence Community Marketplace per la Console.
   b. Nella scheda Avvio personalizzato, seleziona l'opzione per avviare l'istanza dalla console EC2.
   c. Seguire le istruzioni per configurare l'istanza.

      Durante la configurazione dell'istanza, tenere presente quanto segue:

      - Consigliamo t3.xlarge.
      - Devi scegliere il ruolo IAM che hai creato quando hai impostato le autorizzazioni.
      - Dovresti mantenere le opzioni di archiviazione predefinite.
      - I metodi di connessione richiesti per l'agente Console sono i seguenti: SSH, HTTP e HTTPS.
3. Configurare la console da un host che ha una connessione all'istanza:
   a. Apri un browser web e inserisci https://ipaddress dove ipaddress è l’indirizzo IP dell’host Linux in cui è installato l’agente Console.
   b. Specificare un server proxy per la connettività ai servizi AWS.
   c. Carica il certificato ottenuto nel passaggio 1.
   d. Seguire le istruzioni per configurare un nuovo sistema.
      - **Dettagli di sistema**: immettere un nome per l'agente della console e il nome della propria azienda.
      - **Crea utente amministratore**: crea l'utente amministratore per il sistema.

        Questo account utente viene eseguito localmente sul sistema. Non è disponibile alcuna connessione al servizio auth0 tramite la Console.

- **Revisione**: rivedere i dettagli, accettare il contratto di licenza e quindi selezionare **Configura**.

e. Per completare l'installazione del certificato firmato dalla CA, riavviare l'istanza dell'agente Console dalla console EC2.

4. Dopo il riavvio dell'agente Console, effettuare l'accesso utilizzando l'account utente amministratore creato nella procedura guidata di installazione.

Passaggio 5: (facoltativo) Installa un certificato in modalità privata

Questo passaggio è facoltativo per le regioni AWS Secret Cloud e Top Secret Cloud ed è obbligatorio solo se si dispone di certificati aggiuntivi oltre ai certificati radice installati nel passaggio precedente.

Passi

1. Elenca i certificati installati esistenti.
   a. Per raccogliere l'ID Docker del contenitore occm (nome identificato "ds-occm-1"), eseguire il seguente comando:

```
docker ps
```

   b. Per accedere al contenitore occm, eseguire il seguente comando:

```
docker exec -it <docker-id> /bin/sh
```

   c. Per raccogliere la password dalla variabile di ambiente "TRUST_STORE_PASSWORD", eseguire il seguente comando:

```
env
```

   d. Per elencare tutti i certificati installati nel truststore, eseguire il comando seguente e utilizzare la password raccolta nel passaggio precedente:

```
keytool -list -v -keystore occm.truststore
```

2. Aggiungi un certificato.
   a. Per raccogliere l'ID Docker del contenitore occm (nome identificato "ds-occm-1"), eseguire il seguente comando:

```
docker ps
```

   b. Per accedere al contenitore occm, eseguire il seguente comando:

```
docker exec -it <docker-id> /bin/sh
```

Salvare il nuovo file del certificato all'interno.

c. Per raccogliere la password dalla variabile di ambiente "TRUST_STORE_PASSWORD", eseguire il seguente comando:

```
env
```

d. Per aggiungere il certificato al truststore, eseguire il comando seguente e utilizzare la password del passaggio precedente:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. Per verificare che il certificato sia installato, eseguire il seguente comando:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. Per uscire dal contenitore occm, eseguire il seguente comando:

```
exit
```

g. Per reimpostare il contenitore occm, eseguire il seguente comando:

```
docker restart <docker-id>
```

Passaggio 6: aggiungere una licenza alla console

Se hai acquistato una licenza da NetApp, devi aggiungerla alla Console, in modo da poterla selezionare quando crei un nuovo sistema Cloud Volumes ONTAP . Queste licenze rimangono non assegnate finché non vengono associate a un nuovo sistema Cloud Volumes ONTAP .

Passi

1. Dal menu di navigazione a sinistra, seleziona * Licenses and subscriptions*.
2. Nel pannello * Cloud Volumes ONTAP*, selezionare **Visualizza**.
3. Nella scheda * Cloud Volumes ONTAP*, seleziona **Licenze > Licenze basate su nodi**.
4. Fare clic su **Non assegnato**.
5. Fare clic su **Aggiungi licenze non assegnate**.
6. Inserisci il numero di serie della licenza o carica il file della licenza.
7. Se non hai ancora il file di licenza, dovrai caricarlo manualmente da netapp.com.
   a. Vai al"Generatore di file di licenza NetApp" e accedi utilizzando le credenziali del sito di supporto NetApp .

b. Inserisci la tua password, scegli il tuo prodotto, inserisci il numero di serie, conferma di aver letto e accettato l'informativa sulla privacy, quindi clicca su **Invia**.

c. Scegli se desideri ricevere il file JSON serialnumber.NLF tramite e-mail o tramite download diretto.

8. Fare clic su **Aggiungi licenza**.

Risultato

La Console aggiunge la licenza come non assegnata finché non la si associa a un nuovo sistema Cloud Volumes ONTAP . Puoi visualizzare la licenza nel menu di navigazione a sinistra in * Licenses and subscriptions > Cloud Volumes ONTAP > Visualizza > Licenze*.

Passaggio 7: avviare Cloud Volumes ONTAP dalla console

È possibile avviare istanze Cloud Volumes ONTAP in AWS Secret Cloud e Top Secret Cloud creando nuovi sistemi nella Console.

Prima di iniziare

Per le coppie HA, è necessaria una coppia di chiavi per abilitare l'autenticazione SSH basata su chiave al mediatore HA.

Passi

1. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema**.
2. In **Crea**, seleziona Cloud Volumes ONTAP.

   Per HA: in **Crea**, seleziona Cloud Volumes ONTAP o Cloud Volumes ONTAP HA.

3. Completare i passaggi della procedura guidata per avviare il sistema Cloud Volumes ONTAP .

> Durante le selezioni tramite la procedura guidata, non selezionare **Data Sense & Compliance** e **Backup su cloud** in **Servizi**. In **Pacchetti preconfigurati**, seleziona solo **Modifica configurazione** e assicurati di non aver selezionato altre opzioni. I pacchetti preconfigurati non sono supportati nelle regioni AWS Secret Cloud e Top Secret Cloud e, se selezionati, la distribuzione non andrà a buon fine.

Note per la distribuzione di Cloud Volumes ONTAP HA in più zone di disponibilità

Durante il completamento della procedura guidata per le coppie HA, tenere presente quanto segue.

- Quando si distribuisce Cloud Volumes ONTAP HA in più zone di disponibilità (AZ), è necessario configurare un gateway di transito. Per le istruzioni, fare riferimento a"Configurare un gateway di transito AWS" .
- Distribuire la configurazione come segue perché al momento della pubblicazione erano disponibili solo due AZ nell'AWS Top Secret Cloud:
  - Nodo 1: Zona di disponibilità A
  - Nodo 2: Zona di disponibilità B
  - Mediatore: Zona di disponibilità A o B

Note per la distribuzione di Cloud Volumes ONTAP in nodi singoli e HA

Durante il completamento della procedura guidata, tieni presente quanto segue:

- Dovresti lasciare l'opzione predefinita per utilizzare un gruppo di sicurezza generato.

Il gruppo di sicurezza predefinito include le regole di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. Se hai la necessità di utilizzare il tuo, puoi fare riferimento alla sezione relativa al gruppo di sicurezza riportata di seguito.

- Devi scegliere il ruolo IAM che hai creato durante la preparazione del tuo ambiente AWS.
- Il tipo di disco AWS sottostante è per il volume iniziale Cloud Volumes ONTAP .

  È possibile scegliere un tipo di disco diverso per i volumi successivi.

- Le prestazioni dei dischi AWS sono legate alle dimensioni del disco.

  Dovresti scegliere la dimensione del disco che ti garantisce le prestazioni costanti di cui hai bisogno. Per maggiori dettagli sulle prestazioni di EBS, consultare la documentazione AWS.

- La dimensione del disco è la dimensione predefinita per tutti i dischi del sistema.

> Se in seguito avrai bisogno di una dimensione diversa, puoi utilizzare l'opzione Allocazione avanzata per creare un aggregato che utilizzi dischi di una dimensione specifica.

Risultato

Viene avviata l'istanza Cloud Volumes ONTAP . Puoi monitorare i progressi nella pagina **Audit**.

Passaggio 8: installare i certificati di sicurezza per la suddivisione in livelli dei dati

È necessario installare manualmente i certificati di sicurezza per abilitare la suddivisione in livelli dei dati nelle regioni AWS Secret Cloud e Top Secret Cloud.

Prima di iniziare

1. Crea bucket S3.

> Assicurarsi che i nomi dei bucket siano preceduti da `fabric-pool-`. Per esempio `fabric-pool-testbucket` .

2. Conserva i certificati radice che hai installato in `step 4` utile.

Passi

1. Copia il testo dai certificati radice che hai installato in `step 4` .
2. Connettiti in modo sicuro al sistema Cloud Volumes ONTAP tramite la CLI.
3. Installare i certificati radice. Potrebbe essere necessario premere il tasto `ENTER` tasto più volte:

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. Quando richiesto, immettere l'intero testo copiato, incluso e da `----- BEGIN CERTIFICATE -----` A `----- END CERTIFICATE -----` .
5. Conservare una copia del certificato digitale firmato dalla CA per riferimento futuro.
6. Conservare il nome della CA e il numero di serie del certificato.

7. Configurare l'archivio oggetti per le regioni AWS Secret Cloud e Top Secret Cloud: `set -privilege advanced -confirmations off`
8. Eseguire questo comando per configurare l'archivio oggetti.

> Tutti gli Amazon Resource Name (ARN) devono essere suffissati con `-iso-b` , ad esempio `arn:aws-iso-b` . Ad esempio, se una risorsa richiede un ARN con una regione, per Top Secret Cloud, utilizzare la convenzione di denominazione come `us-iso-b` per il `-server` bandiera. Per AWS Secret Cloud, utilizzare `us-iso-b-1` .

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Verificare che l'archivio oggetti sia stato creato correttamente: `storage aggregate object-store show -instance`
10. Collegare l'archivio oggetti all'aggregato. Questa operazione dovrebbe essere ripetuta per ogni nuovo aggregato: `storage aggregate object-store attach -aggregate <aggr1> -object-store -name <S3Bucket>`

Inizia a usare Microsoft Azure

Scopri le opzioni di distribuzione di Cloud Volumes ONTAP in Azure

NetApp offre due opzioni per distribuire Cloud Volumes ONTAP su Azure. Cloud Volumes ONTAP si affida tradizionalmente alla NetApp Console per la distribuzione e l'orchestrazione. A partire da Cloud Volumes ONTAP 9.16.1, puoi sfruttare la distribuzione diretta di Azure Marketplace, un processo semplificato che fornisce accesso a un set limitato, ma comunque potente, di funzionalità e opzioni di Cloud Volumes ONTAP .

Quando distribuisci Cloud Volumes ONTAP direttamente da Azure Marketplace, non è necessario configurare l'agente della console o soddisfare altri criteri di sicurezza e onboarding richiesti per distribuire Cloud Volumes ONTAP tramite la console. Dall'Azure Marketplace puoi distribuire rapidamente Cloud Volumes ONTAP in pochi clic ed esplorare le sue funzionalità e capacità principali nel tuo ambiente.

Una volta completata la distribuzione in Azure Marketplace, è possibile individuare questi sistemi nella Console. Dopo l'individuazione, è possibile gestirli come sistemi Cloud Volumes ONTAP e sfruttare tutte le funzionalità della Console. Fare riferimento a "Scopri i sistemi distribuiti nella Console" .

Ecco il confronto delle funzionalità tra le due opzioni. Si noti che le funzionalità di un'istanza autonoma distribuita tramite Azure Marketplace cambiano quando viene rilevata nella Console.

	Mercato di Azure	NetApp Console
Integrazione	Più breve e più semplice, minima preparazione richiesta per l'impiego diretto	Processo di onboarding più lungo, inclusa l'installazione dell'agente della console
Tipi di macchine virtuali (VM) supportati	Tipi di istanza Eds_v5 e Ls_v3	Gamma completa di tipi di VM.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Configurazioni supportate in Azure"^]
Licenza	Licenza gratuita	Qualsiasi licenza basata sulla capacità."Licenza Cloud Volumes ONTAP"
* Supporto NetApp *	Non incluso	Disponibile, in base al tipo di licenza
Capacità	Fino a 500 GiB	Espandibile tramite configurazione
Modello di distribuzione	Distribuzione in modalità ad alta disponibilità (HA) in una singola zona di disponibilità (AZ)	Tutte le configurazioni supportate, comprese le modalità a nodo singolo e HA, le distribuzioni AZ singole e multiple
Tipo di disco supportato	Dischi gestiti Premium SSD v2	Supporto più ampio."Configurazione predefinita per Cloud Volumes ONTAP"
Velocità di scrittura (modalità di scrittura veloce)	Non supportato	Supportato, in base alla configurazione. "Scopri di più sulle velocità di scrittura in Cloud Volumes ONTAP" .
Capacità di orchestrazione	Non disponibile	Disponibile tramite NetApp Console, in base al tipo di licenza
Numero di VM di archiviazione supportate	Uno per distribuzione	Più VM di archiviazione, in base alla configurazione."Numero supportato di VM di archiviazione"
Modifica del tipo di istanza	Non supportato	Supportato
* Livelli FabricPool *	Non supportato	Supportato

Link correlati

- Distribuzione diretta di Azure Marketplace:"Distribuisci Cloud Volumes ONTAP dal marketplace di Azure"
- Distribuzione tramite la console:"Avvio rapido per Cloud Volumes ONTAP in Azure"
- "Documentazione NetApp Console"

Inizia con NetApp Console

Avvio rapido per Cloud Volumes ONTAP in Azure

Inizia a usare Cloud Volumes ONTAP per Azure in pochi passaggi.

1 Creare un agente Console

Se non hai un "Agente console" eppure devi crearne uno. "Scopri come creare un agente Console in Azure"

Tieni presente che se desideri distribuire Cloud Volumes ONTAP in una subnet in cui non è disponibile l'accesso a Internet, dovrai installare manualmente l'agente Console e accedere alla NetApp Console in esecuzione su tale agente Console. "Scopri come installare manualmente l'agente Console in una posizione senza accesso a Internet"

2 Pianifica la tua configurazione

La Console offre pacchetti preconfigurati che soddisfano i requisiti del tuo carico di lavoro, oppure puoi creare la tua configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione. Per informazioni, fare riferimento a"Pianifica la configurazione Cloud Volumes ONTAP in Azure" .

3 Configura la tua rete

1. Assicurati che la tua VNet e le tue subnet supportino la connettività tra l'agente della console e Cloud Volumes ONTAP.
2. Abilita l'accesso a Internet in uscita dalla VPC di destinazione per NetApp AutoSupport.

   Questo passaggio non è necessario se si distribuisce Cloud Volumes ONTAP in una posizione in cui non è disponibile l'accesso a Internet.

"Scopri di più sui requisiti di rete" .

4 Avvia Cloud Volumes ONTAP

Fare clic su **Aggiungi sistema**, selezionare il tipo di sistema che si desidera distribuire e completare i passaggi della procedura guidata. "Leggi le istruzioni passo passo" .

Link correlati

- "Creazione di un agente Console dalla Console"
- "Creazione di un agente console da Azure Marketplace"
- "Installazione del software dell'agente Console su un host Linux"
- "Cosa fa la Console con i permessi"

Pianifica la configurazione Cloud Volumes ONTAP in Azure

Quando distribuisci Cloud Volumes ONTAP in Azure, puoi scegliere un sistema preconfigurato che soddisfi i requisiti del tuo carico di lavoro oppure puoi creare una configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione.

Scegli una licenza Cloud Volumes ONTAP

Sono disponibili diverse opzioni di licenza per Cloud Volumes ONTAP. Ogni opzione ti consente di scegliere il modello di consumo più adatto alle tue esigenze.

- "Scopri le opzioni di licenza per Cloud Volumes ONTAP"
- "Scopri come impostare le licenze"

Scegli una regione supportata

Cloud Volumes ONTAP è supportato nella maggior parte delle regioni Microsoft Azure. "Visualizza l'elenco completo delle regioni supportate" .

Scegli un tipo di VM supportato

Cloud Volumes ONTAP supporta diversi tipi di VM, a seconda del tipo di licenza scelto.

"Configurazioni supportate per Cloud Volumes ONTAP in Azure"

Comprendere i limiti di archiviazione

Il limite di capacità raw per un sistema Cloud Volumes ONTAP è legato alla licenza. Ulteriori limiti incidono sulle dimensioni degli aggregati e sui volumi. Quando pianifichi la tua configurazione, dovresti essere consapevole di questi limiti.

"Limiti di archiviazione per Cloud Volumes ONTAP in Azure"

Dimensiona il tuo sistema in Azure

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di prestazioni e capacità. Quando si sceglie un tipo di macchina virtuale, un tipo di disco e una dimensione del disco, è necessario tenere presenti alcuni punti chiave:

Tipo di macchina virtuale

Guarda i tipi di macchine virtuali supportati in "Note sulla versione Cloud Volumes ONTAP" e quindi rivedere i dettagli su ciascun tipo di VM supportato. Tieni presente che ogni tipo di VM supporta un numero specifico di dischi dati.

- "Documentazione di Azure: dimensioni delle macchine virtuali per uso generico"
- "Documentazione di Azure: dimensioni delle macchine virtuali con memoria ottimizzata"

Tipo di disco Azure con sistemi a nodo singolo

Quando si creano volumi per Cloud Volumes ONTAP, è necessario scegliere lo storage cloud sottostante che Cloud Volumes ONTAP utilizza come disco.

I sistemi a nodo singolo possono utilizzare questi tipi di Azure Managed Disks:

- I dischi gestiti SSD Premium offrono prestazioni elevate per carichi di lavoro ad alta intensità di I/O a un costo più elevato.
- I dischi gestiti Premium SSD v2 offrono prestazioni più elevate con una latenza inferiore a un costo inferiore rispetto ai dischi gestiti Premium SSD.
- I dischi gestiti SSD standard garantiscono prestazioni costanti per carichi di lavoro che richiedono IOPS bassi.

- I dischi gestiti HDD standard sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

Per ulteriori dettagli sui casi d'uso di questi dischi, fare riferimento a "Documentazione di Microsoft Azure: quali tipi di dischi sono disponibili in Azure?" .

Tipo di disco di Azure con coppie HA

I sistemi HA utilizzano dischi gestiti condivisi Premium SSD, entrambi in grado di garantire prestazioni elevate per carichi di lavoro ad alta intensità di I/O a un costo più elevato. Le distribuzioni HA create prima della versione 9.12.1 utilizzano blob di pagine Premium.

Dimensioni del disco di Azure

Quando si avviano istanze Cloud Volumes ONTAP , è necessario scegliere la dimensione del disco predefinita per gli aggregati. NetApp Console utilizza questa dimensione del disco per l'aggregato iniziale e per tutti gli aggregati aggiuntivi creati quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa da quella predefinita"utilizzando l'opzione di allocazione avanzata" .

Tutti i dischi di un aggregato devono avere le stesse dimensioni.

Quando si sceglie la dimensione del disco, è necessario prendere in considerazione diversi fattori. Le dimensioni del disco influiscono sul costo dell'archiviazione, sulle dimensioni dei volumi che è possibile creare in aggregato, sulla capacità totale disponibile per Cloud Volumes ONTAP e sulle prestazioni di archiviazione.

Le prestazioni di Azure Premium Storage sono legate alle dimensioni del disco. I dischi più grandi garantiscono IOPS e throughput più elevati. Ad esempio, la scelta di dischi da 1 TiB può garantire prestazioni migliori rispetto a dischi da 500 GiB, ma a un costo più elevato.

Non ci sono differenze di prestazioni tra le dimensioni dei dischi per Standard Storage. Dovresti scegliere la dimensione del disco in base alla capacità di cui hai bisogno.

Per informazioni su IOPS e velocità effettiva in base alle dimensioni del disco, fare riferimento ad Azure:

- "Microsoft Azure: prezzi di Managed Disks"
- "Microsoft Azure: prezzi dei Page Blobs"

Visualizza i dischi di sistema predefiniti

Oltre allo storage per i dati utente, la Console acquista anche storage cloud per i dati di sistema Cloud Volumes ONTAP (dati di avvio, dati root, dati core e NVRAM). Ai fini della pianificazione, potrebbe essere utile rivedere questi dettagli prima di distribuire Cloud Volumes ONTAP.

"Visualizza i dischi predefiniti per i dati di sistema Cloud Volumes ONTAP in Azure" .

L'agente Console richiede anche un disco di sistema. "Visualizza i dettagli sulla configurazione predefinita dell'agente della console" .

Raccogliere informazioni di rete

Quando si distribuisce Cloud Volumes ONTAP in Azure, è necessario specificare i dettagli sulla rete virtuale. Puoi utilizzare un foglio di lavoro per raccogliere le informazioni dal tuo amministratore.

Informazioni su Azure	Il tuo valore
Regione	
Rete virtuale (VNet)	
Sottorete	
Gruppo di sicurezza di rete (se ne utilizzi uno tuo)	

Scegli una velocità di scrittura

La console consente di scegliere un'impostazione della velocità di scrittura per Cloud Volumes ONTAP. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normale e alta, nonché i rischi e i consigli relativi all'utilizzo di una velocità di scrittura elevata. "Scopri di più sulla velocità di scrittura" .

Scegli un profilo di utilizzo del volume

ONTAP include diverse funzionalità di efficienza di archiviazione che possono ridurre la quantità totale di spazio di archiviazione necessario. Quando si crea un volume nella Console, è possibile scegliere un profilo che abiliti queste funzionalità oppure un profilo che le disabiliti. Dovresti saperne di più su queste funzionalità per decidere quale profilo utilizzare.

Le funzionalità di efficienza dello storage NetApp offrono i seguenti vantaggi:

Provisioning sottile

Offre agli host o agli utenti più spazio di archiviazione logica di quello effettivamente disponibile nel pool di archiviazione fisico. Invece di preallocare lo spazio di archiviazione, lo spazio di archiviazione viene allocato dinamicamente a ciascun volume man mano che i dati vengono scritti.

Deduplicazione

Migliora l'efficienza individuando blocchi di dati identici e sostituendoli con riferimenti a un singolo blocco condiviso. Questa tecnica riduce i requisiti di capacità di archiviazione eliminando i blocchi ridondanti di dati che risiedono nello stesso volume.

Compressione

Riduce la capacità fisica necessaria per archiviare i dati comprimendoli all'interno di un volume su storage primario, secondario e di archivio.

Configurare la rete di Azure per Cloud Volumes ONTAP

La NetApp Console gestisce la configurazione dei componenti di rete per Cloud Volumes ONTAP, come indirizzi IP, maschere di rete e percorsi. È necessario assicurarsi che l'accesso a Internet in uscita sia disponibile, che siano disponibili sufficienti indirizzi IP privati, che siano attive le connessioni giuste e altro ancora.

Requisiti per Cloud Volumes ONTAP

In Azure devono essere soddisfatti i seguenti requisiti di rete.

Accesso a Internet in uscita

I sistemi Cloud Volumes ONTAP necessitano di accesso a Internet in uscita per accedere agli endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con requisiti di sicurezza rigorosi.

L'agente della console contatta anche diversi endpoint per le operazioni quotidiane. Per informazioni sugli endpoint, fare riferimento a "Visualizza gli endpoint contattati dall'agente della console" E "Preparare la rete per l'utilizzo della console" .

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se non disponibile
\ https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione nella Console.	Modalità standard e limitata.	L'autenticazione dell'utente fallisce e i seguenti servizi rimangono non disponibili: • Servizi Cloud Volumes ONTAP • Servizi ONTAP • Protocolli e servizi proxy
https://vault.azure.net	Deposito chiavi	Utilizzato per recuperare le chiavi segrete del client da Azure Key Vault quando si utilizzano chiavi gestite dal cliente (CMK).	Modalità standard, limitata e privata.	I servizi Cloud Volumes ONTAP non sono disponibili.
\ https://api.bluexp.netapp.com/tenancy	Locazione	Utilizzato per recuperare le risorse Cloud Volumes ONTAP dalla Console per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilizzato per inviare i dati di telemetria AutoSupport al supporto NetApp .	Modalità standard e limitata.	Le informazioni AutoSupport non vengono recapitate.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se non disponibile
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	Regioni pubbliche	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Regione della Cina	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	Regione Germania	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Regioni governative	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	Regioni del Dipartimento della Difesa del governo	Comunicazione con i servizi Azure.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Azure per eseguire operazioni specifiche per la console in Azure.

Configurazione del proxy di rete dell'agente NetApp Console

È possibile utilizzare la configurazione dei server proxy dell'agente NetApp Console per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. La console supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy dell'agente della console. L'amministratore potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato sul sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.
- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP tramite il proxy per l'agente della console. Quando si configura un proxy trasparente, l'amministratore deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurati di ottenere e caricare lo stesso certificato CA radice sul tuo sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy, fare riferimento a "Configurare l'agente della console per utilizzare un server proxy" .

indirizzi IP

La console assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Azure. Devi assicurarti che la tua rete disponga di un numero sufficiente di indirizzi IP privati.

Il numero di LIF allocati per Cloud Volumes ONTAP dipende dal fatto che si distribuisca un sistema a nodo singolo o una coppia HA. Un LIF è un indirizzo IP associato a una porta fisica. Un LIF di gestione SVM è necessario per strumenti di gestione come SnapCenter.

> Un iSCSI LIF fornisce l'accesso client tramite il protocollo iSCSI e viene utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere eliminati.

Indirizzi IP per un sistema a nodo singolo

La NetApp Console assegna 5 o 6 indirizzi IP a un sistema a nodo singolo:

- IP di gestione del cluster
- IP di gestione dei nodi
- IP intercluster per SnapMirror
- IP NFS/CIFS
- IP iSCSI

> L'IP iSCSI fornisce l'accesso client tramite il protocollo iSCSI. Viene utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questo LIF è obbligatorio e non deve essere eliminato.

- Gestione SVM (facoltativa, non configurata di default)

Indirizzi IP per coppie HA

Durante la distribuzione, la console assegna indirizzi IP a 4 NIC (per nodo).

Si noti che la NetApp Console crea un LIF di gestione SVM sulle coppie HA, ma non sui sistemi a nodo singolo in Azure.

NIC0

- IP di gestione dei nodi
- IP intercluster
- IP iSCSI

> L'IP iSCSI fornisce l'accesso client tramite il protocollo iSCSI. Viene utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questo LIF è obbligatorio e non deve essere eliminato.

NIC1

- IP di rete del cluster

NIC2

- IP di interconnessione del cluster (HA IC)

NIC3

- IP NIC Pageblob (accesso al disco)

> NIC3 è applicabile solo alle distribuzioni HA che utilizzano l'archiviazione BLOB di pagina.

Gli indirizzi IP sopra indicati non migrano in caso di eventi di failover.

Inoltre, 4 IP frontend (FIP) sono configurati per migrare in caso di eventi di failover. Questi IP frontend risiedono nel bilanciatore del carico.

- IP di gestione del cluster
- IP dati NodeA (NFS/CIFS)
- IP dati NodeB (NFS/CIFS)
- IP di gestione SVM

Connessioni sicure ai servizi di Azure

Per impostazione predefinita, la console abilita un collegamento privato di Azure per le connessioni tra Cloud Volumes ONTAP e gli account di archiviazione BLOB di pagine di Azure.

Nella maggior parte dei casi, non c'è nulla che tu debba fare: la console gestisce il collegamento privato di Azure per te. Ma se si utilizza Azure Private DNS, sarà necessario modificare un file di configurazione. È inoltre necessario essere a conoscenza di un requisito relativo alla posizione dell'agente della console in Azure.

Se le esigenze aziendali lo richiedono, puoi anche disattivare la connessione Private Link. Se si disabilita il

collegamento, la Console configura Cloud Volumes ONTAP in modo che utilizzi invece un endpoint di servizio.

"Scopri di più sull'utilizzo di Azure Private Links o endpoint di servizio con Cloud Volumes ONTAP" .

Networking per la crittografia di Azure VNet

Cloud Volumes ONTAP supporta "Crittografia di Azure Virtual Network (VNet)" la crittografia del traffico da VM a VM all'interno di una VNet o tra VNets in peering. Questa funzionalità è configurata a livello di VNet di Azure ed è indipendente dalla topologia di Cloud Volumes ONTAP (nodo singolo o HA).

È sufficiente assicurarsi che Accelerated Networking sia abilitato sulle schede di rete della macchina virtuale e verificare i requisiti e le limitazioni di crittografia della rete virtuale di Azure prima di abilitare la funzionalità. Non si devono modificare gli oggetti del servizio di bilanciamento del carico gestito NetApp.

"Documentazione Azure: crittografia VNet e Accelerated Networking".

Collegamenti ad altri sistemi ONTAP

Per replicare i dati tra un sistema Cloud Volumes ONTAP in Azure e sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra la rete virtuale di Azure e l'altra rete, ad esempio la rete aziendale.

Per le istruzioni, fare riferimento al "Documentazione di Microsoft Azure: creare una connessione da sito a sito nel portale di Azure" .

Porta per l'interconnessione HA

Una coppia Cloud Volumes ONTAP HA include un'interconnessione HA, che consente a ciascun nodo di verificare continuamente se il partner funziona e di eseguire il mirroring dei dati di registro per la memoria non volatile dell'altro. L'interconnessione HA utilizza la porta TCP 10006 per la comunicazione.

Per impostazione predefinita, la comunicazione tra i LIF di interconnessione HA è aperta e non sono presenti regole di gruppo di sicurezza per questa porta. Tuttavia, se si crea un firewall tra i LIF di interconnessione HA, è necessario assicurarsi che il traffico TCP sia aperto per la porta 10006, in modo che la coppia HA possa funzionare correttamente.

Solo una coppia HA in un gruppo di risorse di Azure

È necessario utilizzare un gruppo di risorse *dedicato* per ogni coppia Cloud Volumes ONTAP HA distribuita in Azure. In un gruppo di risorse è supportata solo una coppia HA.

La console riscontra problemi di connessione se si tenta di distribuire una seconda coppia Cloud Volumes ONTAP HA in un gruppo di risorse di Azure.

Regole del gruppo di sicurezza

La console crea gruppi di sicurezza di Azure che includono le regole in ingresso e in uscita affinché Cloud Volumes ONTAP funzioni correttamente. "Visualizza le regole del gruppo di sicurezza per l'agente della console" .

I gruppi di sicurezza di Azure per Cloud Volumes ONTAP richiedono che le porte appropriate siano aperte per la comunicazione interna tra i nodi. "Scopri di più sulle porte interne ONTAP" .

Si sconsiglia di modificare i gruppi di sicurezza predefiniti o di utilizzare gruppi di sicurezza personalizzati. Tuttavia, se necessario, tieni presente che il processo di distribuzione richiede che il sistema Cloud Volumes ONTAP abbia accesso completo all'interno della propria subnet. Una volta completata la distribuzione, se si

decide di modificare il gruppo di sicurezza di rete, assicurarsi di mantenere aperte le porte del cluster e le porte di rete HA. Ciò garantisce una comunicazione fluida all'interno del cluster Cloud Volumes ONTAP (comunicazione any-to-any tra i nodi).

Regole in entrata per sistemi a nodo singolo

Quando aggiungi un sistema Cloud Volumes ONTAP e scegli un gruppo di sicurezza predefinito, puoi scegliere di consentire il traffico all'interno di uno dei seguenti:

- **Solo VNet selezionata**: l'origine del traffico in entrata è l'intervallo di subnet della VNet per il sistema Cloud Volumes ONTAP e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata.
- **Tutte le reti virtuali**: l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
- **Disabilitato**: questa opzione limita l'accesso alla rete pubblica al tuo account di archiviazione e disabilita la suddivisione in livelli dei dati per i sistemi Cloud Volumes ONTAP . Questa è un'opzione consigliata se i tuoi indirizzi IP privati non devono essere esposti nemmeno all'interno della stessa rete virtuale a causa delle normative e delle policy di sicurezza.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Da qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione del nodo
1001 in entrata_http	80 TCP	Da qualsiasi a qualsiasi	Accesso HTTP alla console Web di ONTAP System Manager tramite l'indirizzo IP del LIF di gestione del cluster
1002 in entrata_111_tcp	111 TCP	Da qualsiasi a qualsiasi	Chiamata di procedura remota per NFS
1003 in entrata_111_udp	111 UDP	Da qualsiasi a qualsiasi	Chiamata di procedura remota per NFS
1004 in entrata_139	139 TCP	Da qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS
1005 in entrata_161-162 _tcp	161-162 TCP	Da qualsiasi a qualsiasi	Protocollo semplice di gestione della rete
1006 in entrata_161-162 _udp	161-162 UDP	Da qualsiasi a qualsiasi	Protocollo semplice di gestione della rete
1007 in entrata_443	443 TCP	Da qualsiasi a qualsiasi	Connettività con l'agente Console e accesso HTTPS alla console Web ONTAP System Manager utilizzando l'indirizzo IP del LIF di gestione del cluster
1008 in entrata_445	445 TCP	Da qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con framing NetBIOS

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1009 in entrata_635_tcp	635 TCP	Da qualsiasi a qualsiasi	Montaggio NFS
1010 in entrata_635_udp	635 UDP	Da qualsiasi a qualsiasi	Montaggio NFS
1011 in entrata_749	749 TCP	Da qualsiasi a qualsiasi	Kerberos
1012 in entrata_2049_tcp	2049 TCP	Da qualsiasi a qualsiasi	Demone del server NFS
1013 in entrata_2049_udp	2049 UDP	Da qualsiasi a qualsiasi	Demone del server NFS
1014 in entrata_3260	3260 TCP	Da qualsiasi a qualsiasi	Accesso iSCSI tramite i dati iSCSI LIF
1015 in entrata_4045-4046_tcp	4045-4046 TCP	Da qualsiasi a qualsiasi	Demone di blocco NFS e monitor dello stato della rete
1016 in entrata_4045-4046_udp	4045-4046 UDP	Da qualsiasi a qualsiasi	Demone di blocco NFS e monitor dello stato della rete
1017 in entrata_10000	10000 TCP	Da qualsiasi a qualsiasi	Backup tramite NDMP
1018 in entrata_11104-11105	11104-11105 TCP	Da qualsiasi a qualsiasi	Trasferimento dati SnapMirror
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico TCP in entrata
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta Qualsiasi protocollo	Da rete virtuale a rete virtuale	Traffico in entrata dall'interno della VNet
65001 ConsentiAzureLoad BalancerInBound	Qualsiasi porta Qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico dati da Azure Standard Load Balancer
65500 DenyAllInBound	Qualsiasi porta Qualsiasi protocollo	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico in entrata

Regole in entrata per sistemi HA

Quando aggiungi un sistema Cloud Volumes ONTAP e scegli un gruppo di sicurezza predefinito, puoi scegliere di consentire il traffico all'interno di uno dei seguenti:

- **Solo VNet selezionata**: l'origine del traffico in entrata è l'intervallo di subnet della VNet per il sistema Cloud Volumes ONTAP e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata.
- **Tutte le reti virtuali**: l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.

I sistemi HA hanno meno regole in ingresso rispetto ai sistemi a nodo singolo perché il traffico dati in ingresso passa attraverso l'Azure Standard Load Balancer. Per questo motivo, il traffico proveniente dal Load Balancer dovrebbe essere aperto, come mostrato nella regola "AllowAzureLoadBalancerInBound".

- **Disabilitato**: questa opzione limita l'accesso alla rete pubblica al tuo account di archiviazione e disabilita la suddivisione in livelli dei dati per i sistemi Cloud Volumes ONTAP . Questa è un'opzione consigliata se i tuoi indirizzi IP privati non devono essere esposti nemmeno all'interno della stessa rete virtuale a causa delle normative e delle policy di sicurezza.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 in entrata_443	443 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Connettività con l'agente Console e accesso HTTPS alla console Web ONTAP System Manager utilizzando l'indirizzo IP del LIF di gestione del cluster
101 in entrata_111_tcp	111 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Chiamata di procedura remota per NFS
102 in entrata_2049_tcp	2049 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Demone del server NFS
111 inbound_ssh	22 Qualsiasi protocollo	Da qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione del nodo
121 in entrata_53	53 Qualsiasi protocollo	Da qualsiasi a qualsiasi	DNS e CIFS
65000 AllowVnetInBound	Qualsiasi porta Qualsiasi protocollo	Da rete virtuale a rete virtuale	Traffico in entrata dall'interno della VNet
65001 ConsentiAzureLoad BalancerInBound	Qualsiasi porta Qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico dati da Azure Standard Load Balancer
65500 DenyAllInBound	Qualsiasi porta Qualsiasi protocollo	Da qualsiasi a qualsiasi	Blocca tutto il resto del traffico in entrata

Regole in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Porta	Protocollo	Scopo
Tutto	Tutti gli TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	Tutto il traffico in uscita

Regole in uscita avanzate

Se hai bisogno di regole rigide per il traffico in uscita, puoi utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte di Cloud Volumes ONTAP.

La sorgente è l'interfaccia (indirizzo IP) sul sistema Cloud Volumes ONTAP .

Servizio	Porta	Protocollo	Fonte	Destinazione	Scopo
Directory attiva	88	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Autenticazione Kerberos V
	137	UDP	Gestione dei nodi LIF	Foresta di Active Directory	Servizio di denominazione NetBIOS
	138	UDP	Gestione dei nodi LIF	Foresta di Active Directory	Servizio datagramma NetBIOS
	139	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Sessione del servizio NetBIOS
	389	TCP e UDP	Gestione dei nodi LIF	Foresta di Active Directory	LDAP
	445	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	464	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	464	UDP	Gestione dei nodi LIF	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)
	88	TCP	Dati LIF (NFS, CIFS, iSCSI)	Foresta di Active Directory	Autenticazione Kerberos V
	137	UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio di denominazione NetBIOS
	138	UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio datagramma NetBIOS
	139	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Sessione del servizio NetBIOS
	389	TCP e UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	LDAP
	445	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	464	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	464	UDP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)

Servizio	Porta	Protocollo	Fonte	Destinazione	Scopo
AutoSupport	HTTPS	443	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	Gestione dei nodi LIF	Agente console	Invio di messaggi AutoSupport tramite un server proxy sull'agente Console, se non è disponibile una connessione Internet in uscita
Backup di configurazione	HTTP	80	Gestione dei nodi LIF	http://<indirizzo-IP-agente-console>/occm/offboxconfig	Inviare i backup della configurazione all'agente della console. "Documentazione ONTAP" .
DHCP	68	UDP	Gestione dei nodi LIF	DHCP	Client DHCP per la prima configurazione
DHCP	67	UDP	Gestione dei nodi LIF	DHCP	server DHCP
DNS	53	UDP	Gestione dei nodi LIF e dati LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Gestione dei nodi LIF	Server di destinazione	Copia NDMP
SMTP	25	TCP	Gestione dei nodi LIF	Server di posta	Avvisi SMTP, possono essere utilizzati per AutoSupport
SNMP	161	TCP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	161	UDP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	162	TCP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	162	UDP	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
SnapMirror	11104	TCP	Intercluster LIF	LIF intercluster ONTAP	Gestione delle sessioni di comunicazione intercluster per SnapMirror
	11105	TCP	Intercluster LIF	LIF intercluster ONTAP	Trasferimento dati SnapMirror
Registro di sistema	514	UDP	Gestione dei nodi LIF	Server Syslog	Messaggi di inoltro Syslog

Requisiti per l'agente della console

Se non hai ancora creato un agente Console, dovresti anche esaminare i requisiti di rete per l'agente Console.

- "Visualizza i requisiti di rete per l'agente della console"
- "Regole del gruppo di sicurezza in Azure"

Argomenti correlati

- "Verifica la configurazione AutoSupport per Cloud Volumes ONTAP"
- "Scopri di più sulle porte interne ONTAP" .

Configurare Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in Azure

I dati vengono crittografati automaticamente su Cloud Volumes ONTAP in Azure utilizzando Azure Storage Service Encryption con una chiave gestita da Microsoft. Ma puoi anche utilizzare la tua chiave di crittografia seguendo i passaggi descritti in questa pagina.

Panoramica sulla crittografia dei dati

I dati Cloud Volumes ONTAP vengono crittografati automaticamente in Azure utilizzando "Crittografia del servizio di archiviazione di Azure" . L'implementazione predefinita utilizza una chiave gestita da Microsoft. Non è richiesta alcuna configurazione.

Se si desidera utilizzare una chiave gestita dal cliente con Cloud Volumes ONTAP, è necessario completare i seguenti passaggi:

1. Da Azure, crea un archivio chiavi e quindi genera una chiave in tale archivio.
2. Dalla NetApp Console, utilizzare l'API per creare un sistema Cloud Volumes ONTAP che utilizzi la chiave.

Come vengono crittografati i dati

La console utilizza un set di crittografia del disco, che consente la gestione delle chiavi di crittografia con dischi gestiti e non con blob di pagine. Anche tutti i nuovi dischi dati utilizzano lo stesso set di crittografia del disco. Le versioni precedenti utilizzeranno la chiave gestita da Microsoft anziché quella gestita dal cliente.

Dopo aver creato un sistema Cloud Volumes ONTAP configurato per utilizzare una chiave gestita dal cliente, i dati di Cloud Volumes ONTAP vengono crittografati come segue.

Configurazione Cloud Volumes ONTAP	Dischi di sistema utilizzati per la crittografia delle chiavi	Dischi dati utilizzati per la crittografia delle chiavi
Nodo singolo	• Stivale • Nucleo • NVRAM	• Radice • Dati
Zona di disponibilità singola di Azure HA con blob di pagine	• Stivale • Nucleo • NVRAM	Nessuno

Configurazione Cloud Volumes ONTAP	Dischi di sistema utilizzati per la crittografia delle chiavi	Dischi dati utilizzati per la crittografia delle chiavi
Zona di disponibilità singola di Azure HA con dischi gestiti condivisi	• Stivale • Nucleo • NVRAM	• Radice • Dati
Zone di disponibilità multiple di Azure HA con dischi gestiti condivisi	• Stivale • Nucleo • NVRAM	• Radice • Dati

Tutti gli account di archiviazione di Azure per Cloud Volumes ONTAP vengono crittografati tramite una chiave gestita dal cliente. Se si desidera crittografare gli account di archiviazione durante la loro creazione, è necessario creare e fornire l'ID della risorsa nella richiesta di creazione Cloud Volumes ONTAP . Questo vale per tutti i tipi di distribuzioni. Se non lo fornisci, gli account di archiviazione saranno comunque crittografati, ma la Console crea prima gli account di archiviazione con la crittografia della chiave gestita da Microsoft e poi aggiorna gli account di archiviazione per utilizzare la chiave gestita dal cliente.

Rotazione delle chiavi in Cloud Volumes ONTAP

Quando si configurano le chiavi di crittografia, è necessario utilizzare il portale di Azure per impostare e abilitare la rotazione automatica delle chiavi. La creazione e l'abilitazione di una nuova versione delle chiavi di crittografia garantisce che Cloud Volumes ONTAP possa rilevare e utilizzare automaticamente la versione più recente della chiave per la crittografia, garantendo la sicurezza dei dati senza la necessità di un intervento manuale.

Per informazioni sulla configurazione delle chiavi e sull'impostazione della rotazione delle chiavi, fare riferimento ai seguenti argomenti della documentazione di Microsoft Azure:

- "Configurare la rotazione automatica delle chiavi crittografiche in Azure Key Vault"
- "Azure PowerShell - Abilita le chiavi gestite dal cliente"

> Dopo aver configurato le chiavi, assicurati di aver selezionato "*Abilita rotazione automatica*" , in modo che Cloud Volumes ONTAP possa utilizzare le nuove chiavi quando quelle precedenti scadono. Se non si abilita questa opzione nel portale di Azure, Cloud Volumes ONTAP non potrà rilevare automaticamente le nuove chiavi, il che potrebbe causare problemi con il provisioning dello storage.

Creare un'identità gestita assegnata dall'utente

Hai la possibilità di creare una risorsa denominata identità gestita assegnata dall'utente. In questo modo è possibile crittografare gli account di archiviazione quando si crea un sistema Cloud Volumes ONTAP . Si consiglia di creare questa risorsa prima di creare un archivio chiavi e generare una chiave.

La risorsa ha il seguente ID: `userassignedidentity` .

Passi

1. In Azure, vai a Servizi di Azure e seleziona **Identità gestite**.
2. Fare clic su **Crea**.

3. Fornire i seguenti dettagli:
   - **Abbonamento**: Scegli un abbonamento. Si consiglia di scegliere lo stesso abbonamento dell'agente della Console.
   - **Gruppo di risorse**: utilizza un gruppo di risorse esistente o creane uno nuovo.
   - **Regione**: facoltativamente, selezionare la stessa regione dell'agente Console.
   - **Nome**: inserisci un nome per la risorsa.
4. Facoltativamente, aggiungi dei tag.
5. Fare clic su **Crea**.

Crea un archivio di chiavi e genera una chiave

L'archivio delle chiavi deve risiedere nella stessa sottoscrizione e regione di Azure in cui si prevede di creare il sistema Cloud Volumes ONTAP .

Se tuha creato un'identità gestita assegnata dall'utente durante la creazione del key vault, dovresti anche creare una policy di accesso per il key vault.

Passi

1. "Crea un archivio chiavi nel tuo abbonamento Azure" .

   Tenere presente i seguenti requisiti per il key vault:

   - Il key vault deve risiedere nella stessa regione del sistema Cloud Volumes ONTAP .
   - Dovrebbero essere abilitate le seguenti opzioni:
     - **Eliminazione temporanea** (questa opzione è abilitata per impostazione predefinita, ma *non* deve essere disabilitata)
     - **Protezione anti-spurgo**
     - **Azure Disk Encryption per la crittografia dei volumi** (per sistemi a nodo singolo, coppia HA in più zone e distribuzioni HA in una sola zona di disponibilità)

       L'utilizzo delle chiavi di crittografia gestite dal cliente di Azure è subordinato all'abilitazione della crittografia del disco di Azure per l'insieme di credenziali delle chiavi.
   - Se hai creato un'identità gestita assegnata dall'utente, dovresti abilitare la seguente opzione:
     - **Politica di accesso al caveau**
2. Se hai selezionato Criterio di accesso al vault, fai clic su Crea per creare un criterio di accesso per il vault delle chiavi. In caso contrario, passare al passaggio 3.
   a. Selezionare le seguenti autorizzazioni:
      - Ottenere
      - lista
      - decifrare
      - crittografare
      - chiave di scarto
      - chiave di avvolgimento

- verificare
- cartello

b. Selezionare l'identità gestita (risorsa) assegnata dall'utente come principale.

c. Rivedere e creare la policy di accesso.

3. "Genera una chiave nel key vault" .

   Notare i seguenti requisiti per la chiave:

   - Il tipo di chiave deve essere **RSA**.
   - La dimensione consigliata della chiave RSA è **2048**, ma sono supportate anche altre dimensioni.

Creare un sistema che utilizzi la chiave di crittografia

Dopo aver creato il key vault e generato una chiave di crittografia, è possibile creare un nuovo sistema Cloud Volumes ONTAP configurato per utilizzare la chiave. Questi passaggi sono supportati tramite l'API.

Autorizzazioni richieste

Se si desidera utilizzare una chiave gestita dal cliente con un sistema Cloud Volumes ONTAP a nodo singolo, assicurarsi che l'agente della console disponga delle seguenti autorizzazioni:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Visualizza l'elenco più recente delle autorizzazioni"

Passi

1. Ottieni l'elenco degli archivi di chiavi nella tua sottoscrizione di Azure utilizzando la seguente chiamata API.

   Per una coppia HA: `GET /azure/ha/metadata/vaults`

   Per nodo singolo: `GET /azure/vsa/metadata/vaults`

   Prendi nota di **nome** e **resourceGroup**. Sarà necessario specificare tali valori nel passaggio successivo.

   "Scopri di più su questa chiamata API" .

2. Ottieni l'elenco delle chiavi all'interno del vault utilizzando la seguente chiamata API.

   Per una coppia HA: `GET /azure/ha/metadata/keys-vault`

   Per nodo singolo: `GET /azure/vsa/metadata/keys-vault`

   Prendi nota di **keyName**. Sarà necessario specificare tale valore (insieme al nome del vault) nel passaggio successivo.

"Scopri di più su questa chiamata API" .

3. Creare un sistema Cloud Volumes ONTAP utilizzando la seguente chiamata API.

   a. Per una coppia HA:

      `POST /azure/ha/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      Includi il `"userAssignedIdentity": " userAssignedIdentityId"` campo se hai creato questa risorsa per utilizzarla per la crittografia dell'account di archiviazione.

      "Scopri di più su questa chiamata API" .

   b. Per un sistema a nodo singolo:

      `POST /azure/vsa/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      Includi il `"userAssignedIdentity": " userAssignedIdentityId"` campo se hai creato questa risorsa per utilizzarla per la crittografia dell'account di archiviazione.

"Scopri di più su questa chiamata API" .

Risultato

Hai un nuovo sistema Cloud Volumes ONTAP configurato per utilizzare la chiave gestita dal cliente per la crittografia dei dati.

Configurare le licenze per Cloud Volumes ONTAP in Azure

Dopo aver deciso quale opzione di licenza utilizzare con Cloud Volumes ONTAP, sono necessari alcuni passaggi prima di poter scegliere tale opzione di licenza durante la creazione di un nuovo sistema.

Freemium

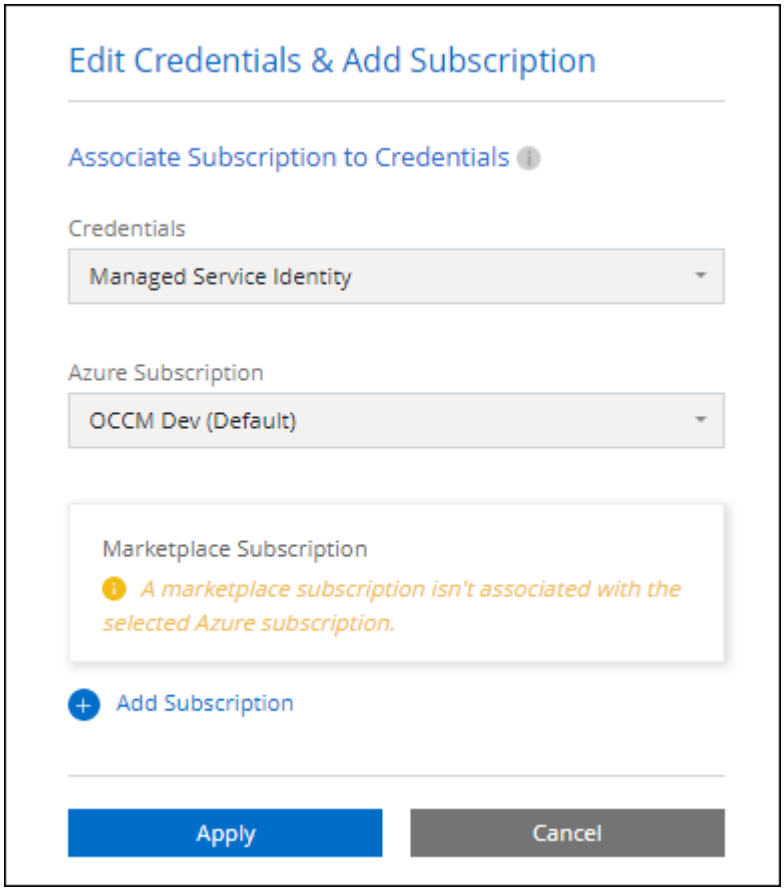
Seleziona l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con una capacità fornita fino a 500 GiB. "Scopri di più sull'offerta Freemium" .

Passi

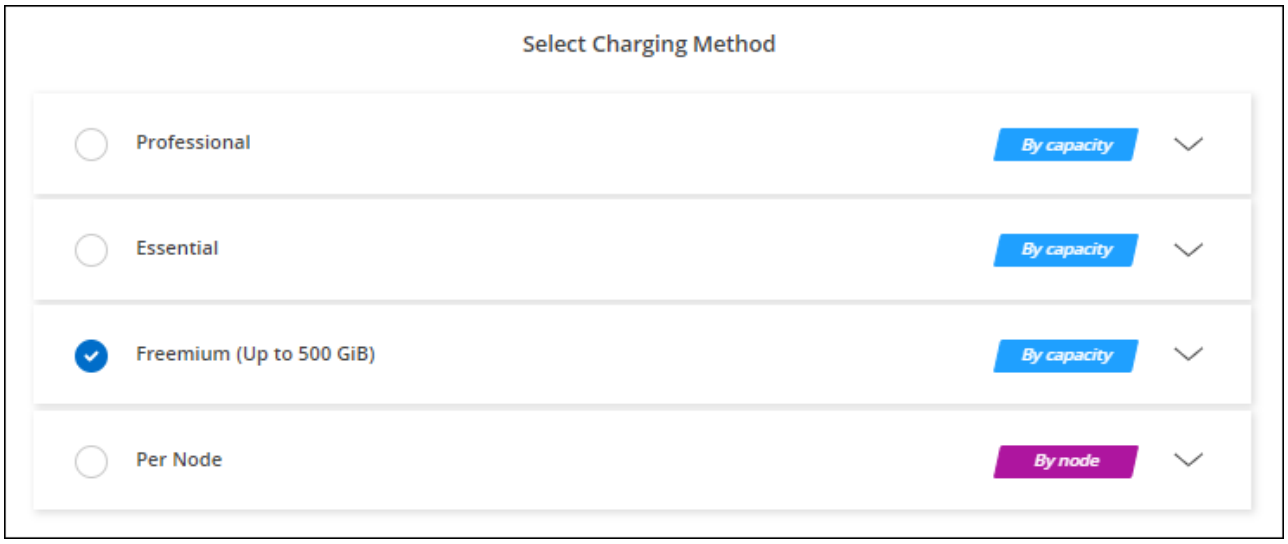
1. Dal menu di navigazione a sinistra della NetApp Console, selezionare **Storage > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.

    a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi sottoscrizione** e quindi seguire le istruzioni per sottoscrivere l'offerta con pagamento in base al consumo in Azure Marketplace.

    Non ti verrà addebitato alcun costo tramite l'abbonamento al marketplace a meno che tu non superi i 500 GiB di capacità fornita, momento in cui il sistema verrà automaticamente convertito in"Pacchetto essenziale" .



    a. Dopo essere tornato alla Console, seleziona **Freemium** quando arrivi alla pagina dei metodi di addebito.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Licenza basata sulla capacità

Le licenze basate sulla capacità consentono di pagare Cloud Volumes ONTAP per TiB di capacità. Le licenze basate sulla capacità sono disponibili sotto forma di *pacchetto*: il pacchetto Essentials o il pacchetto Professional.

I pacchetti Essentials e Professional sono disponibili con i seguenti modelli di consumo o opzioni di acquisto:

- Una licenza (Bring Your Own License (BYOL)) acquistata da NetApp
- Un abbonamento orario con pagamento in base al consumo (PAYGO) da Azure Marketplace
- Un contratto annuale

"Scopri di più sulle licenze basate sulla capacità" .

Le sezioni seguenti descrivono come iniziare a utilizzare ciascuno di questi modelli di consumo.

BYOL

Paga in anticipo acquistando una licenza (BYOL) da NetApp per distribuire i sistemi Cloud Volumes ONTAP in qualsiasi provider cloud.

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Passi

1. "Contatta NetApp Sales per ottenere una licenza"
2. "Aggiungi il tuo account del sito di supporto NetApp alla console"

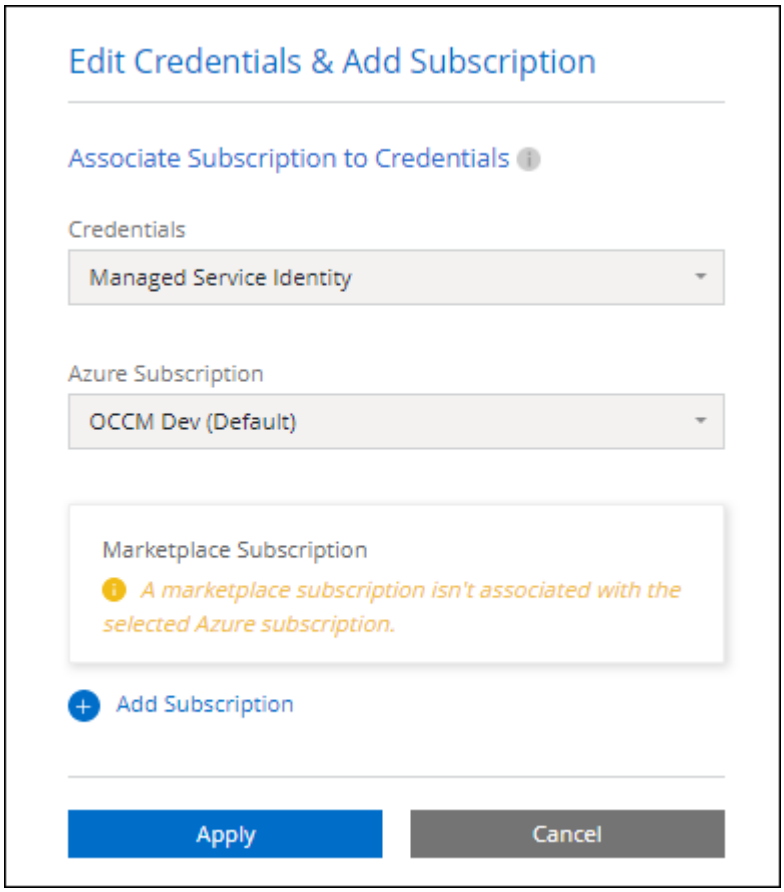
   La Console interroga automaticamente il servizio licenze di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. Se non ci sono errori, la Console aggiunge automaticamente le licenze alla Console.

   La licenza deve essere disponibile nella Console prima di poterla utilizzare con Cloud Volumes ONTAP. Se necessario, puoi"aggiungere manualmente la licenza alla Console" .

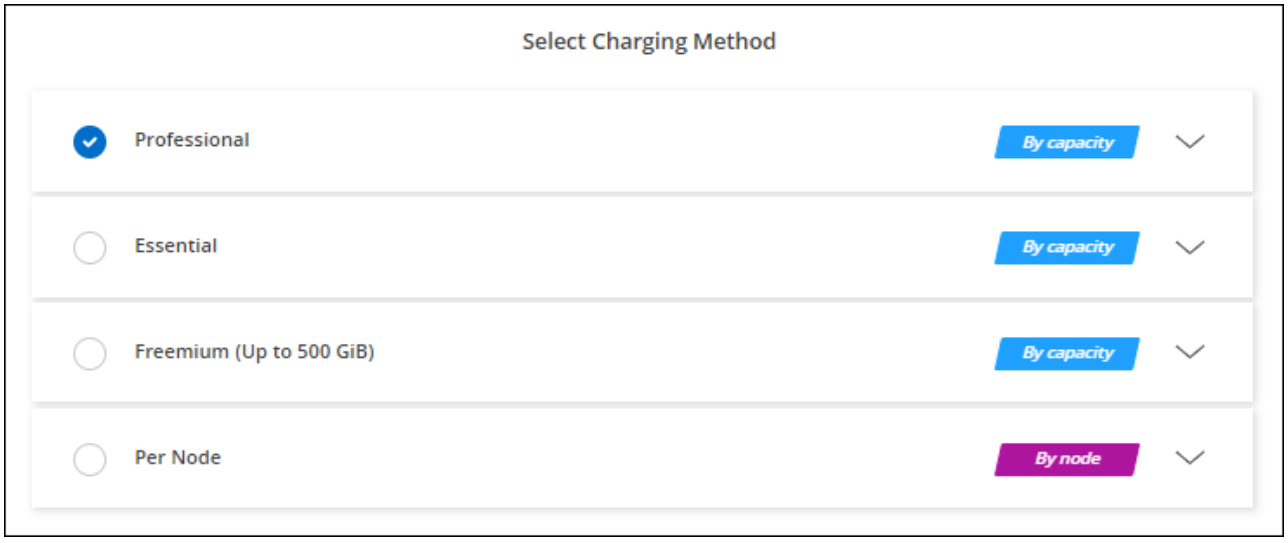
3. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.

   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi sottoscrizione** e quindi seguire le istruzioni per sottoscrivere l'offerta con pagamento in base al consumo in Azure Marketplace.

      La licenza acquistata da NetApp viene sempre addebitata per prima, ma ti verrà addebitata la tariffa oraria del marketplace se superi la capacità della licenza o se scade il termine della licenza.



   a. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

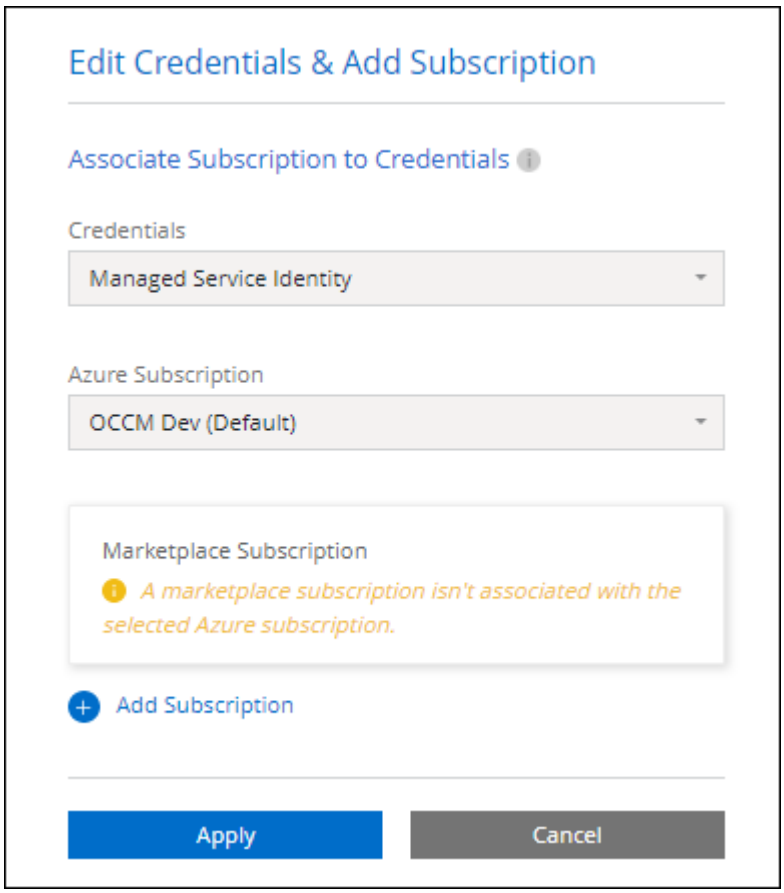
Abbonamento PAYGO

Paga a ore sottoscrivendo l'offerta dal marketplace del tuo provider cloud.

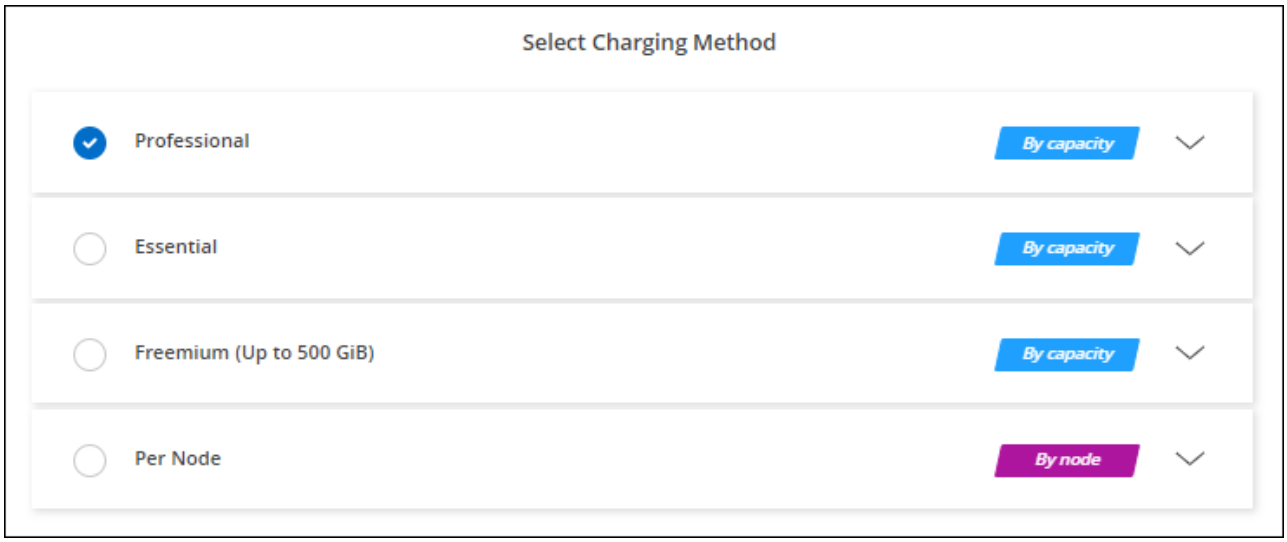
Quando si crea un sistema Cloud Volumes ONTAP , la Console richiede di sottoscrivere il contratto disponibile in Azure Marketplace. Tale abbonamento viene poi associato al sistema di addebito. È possibile utilizzare lo stesso abbonamento per sistemi aggiuntivi.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi sottoscrizione** e quindi seguire le istruzioni per sottoscrivere l'offerta con pagamento in base al consumo in Azure Marketplace.



   b. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Puoi gestire gli abbonamenti di Azure Marketplace associati ai tuoi account Azure dalla pagina Impostazioni > Credenziali. "Scopri come gestire i tuoi account e abbonamenti Azure"

Contratto annuale

Paga annualmente Cloud Volumes ONTAP acquistando un contratto annuale.

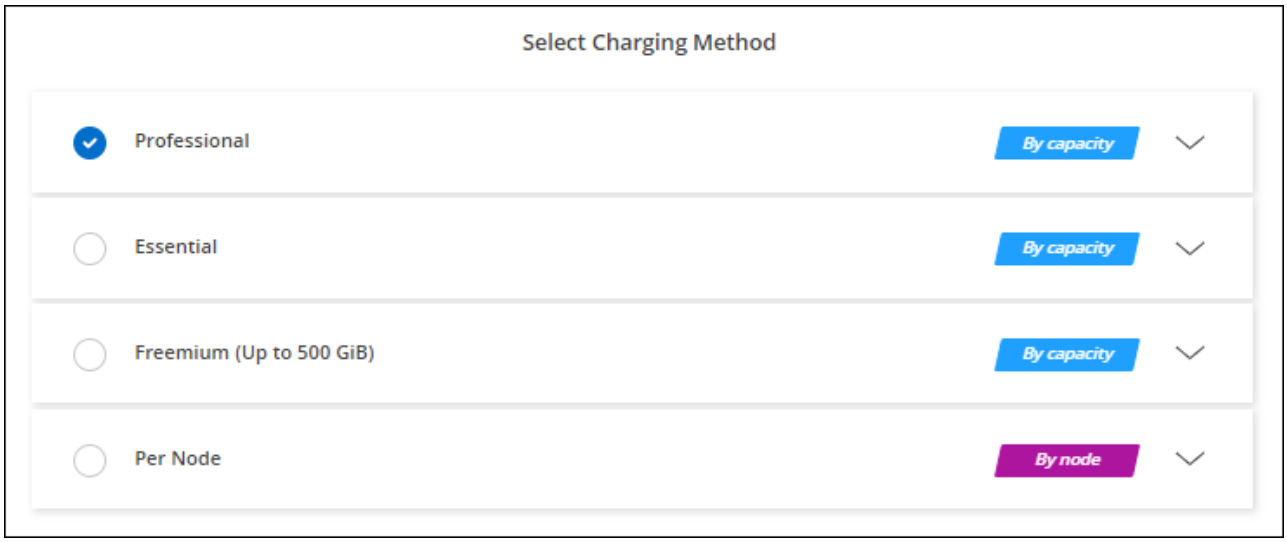
Passi

1. Contatta il tuo rappresentante commerciale NetApp per acquistare un contratto annuale.

   Il contratto è disponibile come offerta *privata* in Azure Marketplace.

   Dopo che NetApp avrà condiviso con te l'offerta privata, potrai selezionare il piano annuale quando ti iscrivi da Azure Marketplace durante la creazione del sistema.

2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento > Continua**.
   b. Nel portale di Azure, seleziona il piano annuale condiviso con il tuo account Azure, quindi fai clic su **Sottoscrivi**.
   c. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



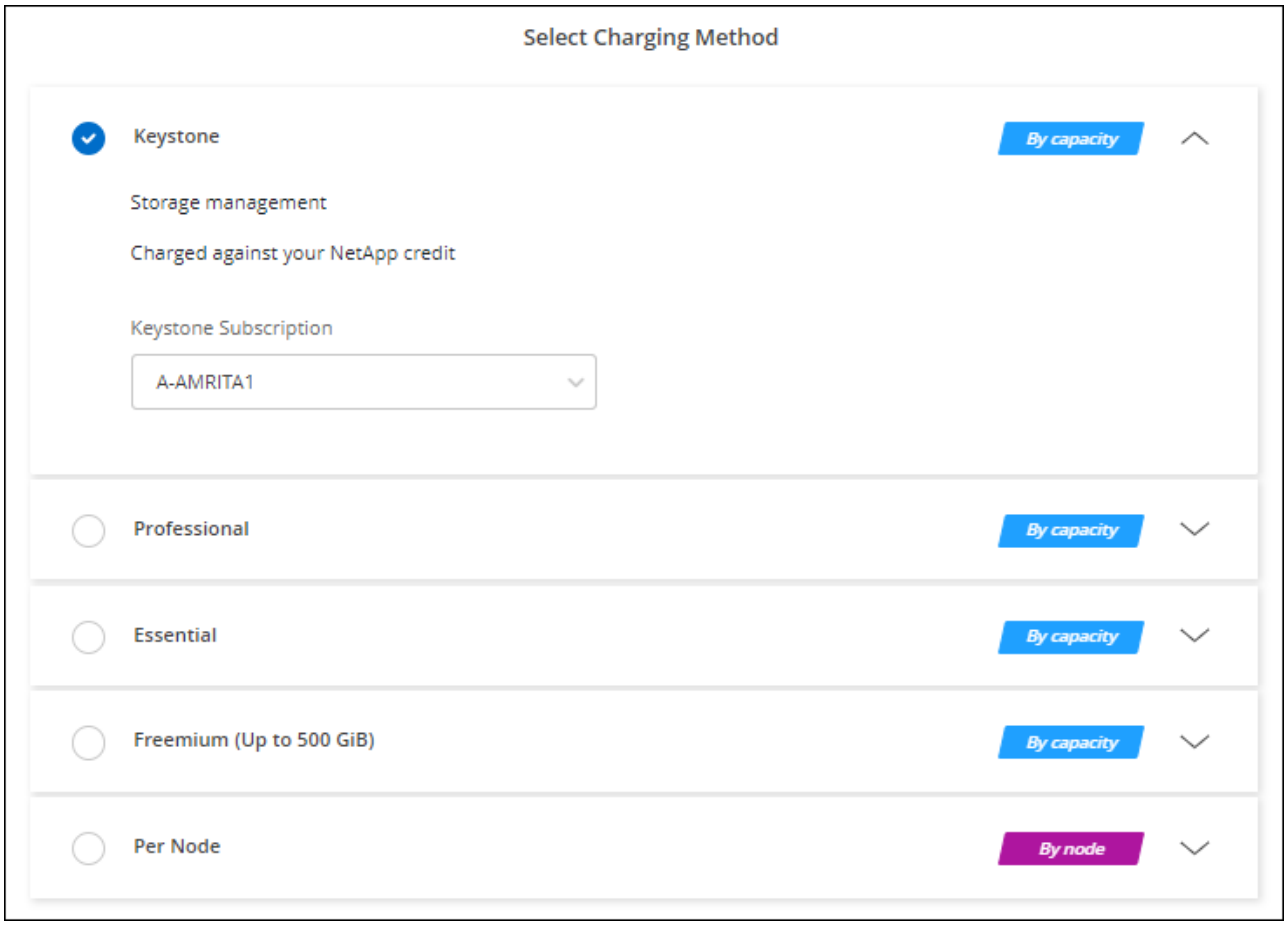
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Abbonamento Keystone

Un abbonamento Keystone è un servizio basato su un abbonamento con pagamento in base alla crescita. "Scopri di più sugli abbonamenti NetApp Keystone" .

Passi

1. Se non hai ancora un abbonamento, "contattare NetApp"
2. Contatta NetApp per autorizzare il tuo account utente nella Console con uno o più abbonamenti Keystone .
3. Dopo che NetApp autorizza il tuo account,"collega i tuoi abbonamenti per utilizzarli con Cloud Volumes ONTAP" .
4. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Quando ti viene richiesto di scegliere un metodo di addebito, seleziona il metodo di addebito Keystone Subscription.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure" .

Licenza basata su nodi

Una licenza basata su nodi è la licenza di precedente generazione per Cloud Volumes ONTAP. Una licenza basata su nodi può essere acquistata da NetApp (BYOL) ed è disponibile per i rinnovi di licenza solo in casi specifici. Per informazioni, fare riferimento a:

- "Fine della disponibilità delle licenze basate su nodi"
- "Fine della disponibilità delle licenze basate sui nodi"
- "Convertire una licenza basata su nodi in una licenza basata sulla capacità"

Abilita la modalità ad alta disponibilità per Cloud Volumes ONTAP in Azure

È consigliabile abilitare la modalità ad alta disponibilità (HA) di Microsoft Azure per ridurre i tempi di failover non pianificati e abilitare il supporto NFSv4 per Cloud Volumes ONTAP. Se abiliti questa modalità, i nodi HA di Cloud Volumes ONTAP possono raggiungere un recovery time objective (RTO) basso (60 secondi) durante i failover non pianificati sui client CIFS e NFSv4.

A partire da Cloud Volumes ONTAP 9.10.1, abbiamo ridotto il tempo di failover non pianificato per le coppie Cloud Volumes ONTAP HA in esecuzione in Microsoft Azure e aggiunto il supporto per NFSv4. Per rendere disponibili questi miglioramenti a Cloud Volumes ONTAP, è necessario abilitare la funzionalità di alta disponibilità nella sottoscrizione di Azure.

Informazioni su questo compito

NetApp Console ti richiede questi dettagli quando la funzionalità deve essere abilitata su un abbonamento Azure. Nota quanto segue:

- Non ci sono problemi con l'elevata disponibilità della coppia Cloud Volumes ONTAP HA. Questa funzionalità di Azure interagisce con ONTAP per ridurre i tempi di interruzione delle applicazioni osservati dal client per i protocolli NFS, derivanti da eventi di failover non pianificati.
- L'abilitazione di questa funzionalità non comporta interruzioni per le coppie Cloud Volumes ONTAP HA.
- L'abilitazione di questa funzionalità nell'abbonamento Azure non causa problemi alle altre VM.
- Cloud Volumes ONTAP utilizza un Azure Load Balancer interno durante i failover dei LIF di gestione del cluster e SVM sui client CIFS e NFS.
- Quando la modalità HA è abilitata, la console esegue la scansione del sistema ogni 12 ore per aggiornare le regole interne di Azure Load Balancer.

Passi

Un utente Azure con privilegi di *Owner* può abilitare la funzionalità dall'Azure CLI.

1. "Accedi ad Azure Cloud Shell dal portale di Azure"
2. Registra la funzionalità della modalità ad alta disponibilità:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Facoltativamente, verificare che la funzionalità sia ora registrata:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

L'interfaccia della riga di comando di Azure dovrebbe restituire un risultato simile al seguente:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Link correlati

1. "Microsoft Azure documentation: panoramica delle porte ad alta disponibilità"
2. "Microsoft Azure documentazione: Introduzione all'Azure CLI"

Abilita VMOrchestratorZonalMultiFD per Cloud Volumes ONTAP in Azure

Per distribuire istanze di VM in zone di disponibilità singole (AZ) con archiviazione ridondante locale (LRS), è necessario attivare Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` funzionalità per i tuoi abbonamenti. In modalità ad alta disponibilità (HA), questa funzionalità semplifica la distribuzione dei nodi in domini di errore separati nella stessa zona di disponibilità.

Se non si attiva questa funzionalità, la distribuzione zonale non avviene e diventa effettiva la precedente distribuzione non zonale LRS.

Per informazioni sulla distribuzione delle VM in una singola zona di disponibilità, fare riferimento a"Coppie ad alta disponibilità in Azure" .

Eseguire questi passaggi come utente con privilegi di "Proprietario":

Passi

1. Accedi ad Azure Cloud Shell dal portale di Azure. Per informazioni fare riferimento al "Documentazione di Microsoft Azure: Introduzione ad Azure Cloud Shell" .
2. Registrati per il `Microsoft.Compute/VMOrchestratorZonalMultiFD` funzionalità eseguendo questo comando:

   ```
   az account set -s <nome_o_ID_abbonamento_Azure> az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. Verificare lo stato della registrazione e il campione di output:

   ```
   az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id": "/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "Registrato" }, "type": "Microsoft.Features/providers/features" }
   ```

Avvia Cloud Volumes ONTAP in Azure

È possibile avviare un sistema a nodo singolo o una coppia HA in Azure creando un sistema Cloud Volumes ONTAP nella NetApp Console.

Prima di iniziare

Prima di iniziare, ti occorre quanto segue.

- Un agente Console attivo e funzionante.
  - Dovresti avere un "Agente console associato al tuo sistema" .
  - "Dovresti essere pronto a lasciare l'agente della console sempre in esecuzione" .

- Una comprensione della configurazione che si desidera utilizzare.

  Dovresti farti fornire dall'amministratore una configurazione pianificata e i dettagli necessari sulla rete di Azure. Per ulteriori informazioni, fare riferimento a "Pianificazione della configurazione Cloud Volumes ONTAP" .

- Una comprensione di ciò che è necessario per impostare la licenza per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze" .

Informazioni su questo compito

Quando la console crea un sistema Cloud Volumes ONTAP in Azure, crea diversi oggetti di Azure, ad esempio un gruppo di risorse, interfacce di rete e account di archiviazione. Alla fine della procedura guidata è possibile visualizzare un riepilogo delle risorse.

> **Potenziale di perdita di dati**
>
> La procedura consigliata è quella di utilizzare un nuovo gruppo di risorse dedicato per ciascun sistema Cloud Volumes ONTAP .
>
> Si sconsiglia di distribuire Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente a causa del rischio di perdita di dati. Sebbene la Console possa rimuovere le risorse Cloud Volumes ONTAP da un gruppo di risorse condivise in caso di errore di distribuzione o eliminazione, un utente di Azure potrebbe eliminare accidentalmente le risorse Cloud Volumes ONTAP da un gruppo di risorse condivise.

Avvia un sistema Cloud Volumes ONTAP a nodo singolo in Azure

Se si desidera avviare un sistema Cloud Volumes ONTAP a nodo singolo in Azure, è necessario creare un sistema a nodo singolo nella Console.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire le istruzioni.
3. **Scegli una posizione**: seleziona **Microsoft Azure** e * Cloud Volumes ONTAP Single Node*.
4. Se richiesto, "creare un agente Console" .
5. **Dettagli e credenziali**: facoltativamente, modifica le credenziali e la sottoscrizione di Azure, specifica un nome per il cluster, aggiungi tag se necessario e quindi specifica le credenziali.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia la macchina virtuale di Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.

Campo	Descrizione
Tag del gruppo di risorse	I tag sono metadati per le risorse di Azure. Quando si immettono tag in questo campo, la Console li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP . Quando si crea un sistema, è possibile aggiungere fino a quattro tag dall'interfaccia utente, per poi aggiungerne altri dopo la creazione. Tieni presente che l'API non ti limita a quattro tag quando crei un sistema. Per informazioni sui tag, fare riferimento a "Documentazione di Microsoft Azure: utilizzo dei tag per organizzare le risorse di Azure" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP . Per distribuire un sistema Cloud Volumes ONTAP con pagamento in base al consumo, è necessario associare una sottoscrizione di Azure Marketplace alla sottoscrizione di Azure selezionata. "Scopri come aggiungere le credenziali" .

6. **Servizi**: abilita o disabilita i singoli servizi che desideri o non desideri utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla NetApp Data Classification"
   - "Scopri di più su NetApp Backup and Recovery"

   Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

7. **Posizione**: selezionare una regione, una zona di disponibilità, una rete virtuale e una subnet, quindi selezionare la casella di controllo per confermare la connettività di rete tra l'agente della console e la posizione di destinazione.

   Per le regioni della Cina, le distribuzioni a nodo singolo sono supportate solo in Cloud Volumes ONTAP 9.12.1 GA e 9.13.0 GA. È possibile aggiornare queste versioni a patch e release successive di Cloud Volumes ONTAP come"supportato in Azure" . Se desideri distribuire versioni successive di Cloud Volumes ONTAP nelle regioni della Cina, contatta l'assistenza NetApp . Nelle regioni della Cina sono supportate solo le licenze acquistate direttamente da NetApp ; gli abbonamenti al marketplace non sono disponibili.

8. **Connettività**: scegli un gruppo di risorse nuovo o esistente e poi scegli se utilizzare il gruppo di sicurezza predefinito o il tuo.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Gruppo di risorse	Crea un nuovo gruppo di risorse per Cloud Volumes ONTAP oppure utilizza un gruppo di risorse esistente. La procedura consigliata è quella di utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile distribuire Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, questa operazione non è consigliata a causa del rischio di perdita di dati. Per maggiori dettagli, vedere l'avviso sopra. Se l'account Azure che stai utilizzando ha il "permessi richiesti" , la Console rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di distribuzione o eliminazione.
Gruppo di sicurezza generato	Se lasci che sia la Console a generare il gruppo di sicurezza per te, devi scegliere come consentire il traffico: • Se si sceglie **Solo VNet selezionata**, l'origine del traffico in entrata è l'intervallo di subnet della VNet selezionata e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le reti virtuali**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizzare esistente	Se si sceglie un gruppo di sicurezza esistente, questo deve soddisfare i requisiti di Cloud Volumes ONTAP . "Visualizza il gruppo di sicurezza predefinito" .

9. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp .
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP" .
   - "Scopri come impostare le licenze" .
10. **Pacchetti preconfigurati**: seleziona uno dei pacchetti per distribuire rapidamente un sistema Cloud Volumes ONTAP oppure fai clic su **Crea la mia configurazione**.

    Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

11. **Licenze**: se necessario, modifica la versione di Cloud Volumes ONTAP e seleziona un tipo di macchina virtuale.

    Se per la versione selezionata è disponibile una versione Release Candidate, una versione General Availability o una patch più recente, BlueXP aggiorna il sistema a tale versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.16.1 P3 e 9.16.1 P4 è disponibile. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.15 alla 9.16.

12. **Iscriviti da Azure Marketplace**: questa pagina viene visualizzata se la console non è riuscita ad abilitare le distribuzioni programmatiche di Cloud Volumes ONTAP. Seguire i passaggi elencati sullo schermo. fare riferimento a "Distribuzione programmatica dei prodotti Marketplace" per maggiori informazioni.
13. **Risorse di archiviazione sottostanti**: scegli le impostazioni per l'aggregato iniziale: un tipo di disco, una

dimensione per ciascun disco e se abilitare la suddivisione dei dati in livelli nell'archiviazione BLOB.

Notare quanto segue:

- Se l'accesso pubblico al tuo account di archiviazione è disabilitato all'interno della VNet, non puoi abilitare la suddivisione in livelli dei dati nel tuo sistema Cloud Volumes ONTAP . Per informazioni, fare riferimento a"Regole del gruppo di sicurezza" .
- Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.
- La dimensione del disco si riferisce a tutti i dischi nell'aggregato iniziale e a tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.

  Per assistenza nella scelta del tipo e della dimensione del disco, fare riferimento a"Dimensionamento del sistema in Azure" .

- Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
- Se si disabilita la suddivisione in livelli dei dati, è possibile abilitarla sugli aggregati successivi.

  "Scopri di più sulla suddivisione in livelli dei dati" .

14. **Velocità di scrittura e WORM**:

    a. Se lo desideri, seleziona la velocità di scrittura **Normale** o **Alta**.

       "Scopri di più sulla velocità di scrittura" .

    b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

       Questa opzione è disponibile solo per alcuni tipi di VM. Per scoprire quali tipi di VM sono supportati, fare riferimento a"Configurazioni supportate per licenza per coppie HA" .

       WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

    "Scopri di più sullo storage WORM" .

    a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.

15. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

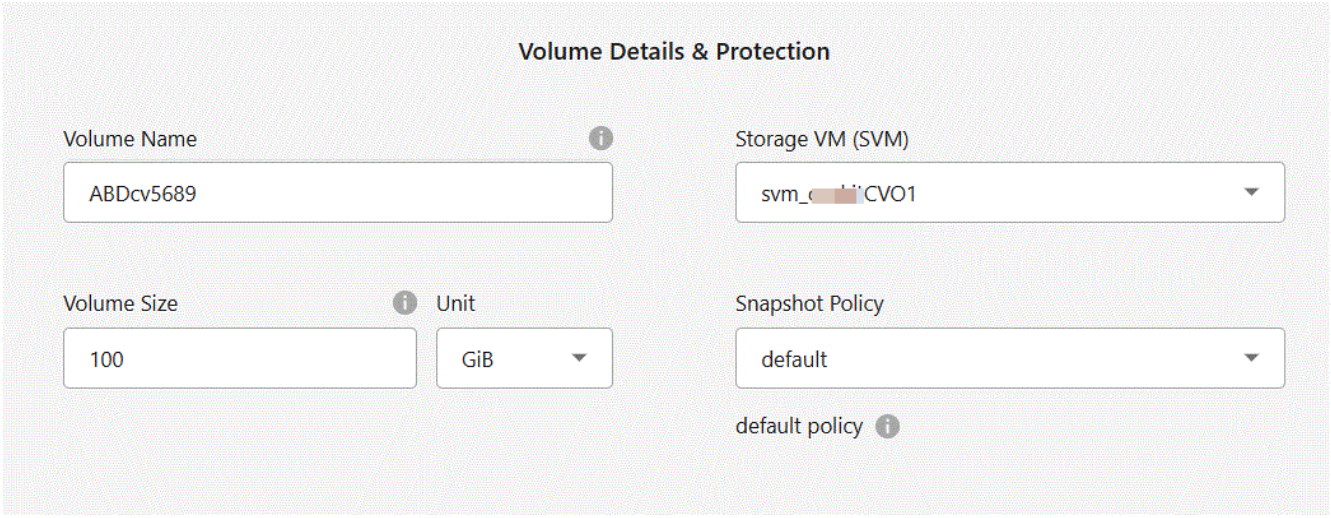
    "Scopri i protocolli e le versioni client supportati" .

    Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.

Campo	Descrizione
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



16. **Configurazione CIFS**: se hai scelto il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Per configurare Azure AD Domain Services come server AD per Cloud Volumes ONTAP, è necessario immettere **OU=Computer AADDC** o **OU=Utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: creare un'unità organizzativa (OU) in un dominio gestito da Azure AD Domain Services"^]
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

17. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Comprensione dei profili di utilizzo del volume" E"Panoramica della suddivisione in livelli dei dati" .

18. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fare clic su **Ulteriori informazioni** per esaminare i dettagli sul supporto e sulle risorse di Azure che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console distribuisce il sistema Cloud Volumes ONTAP . È possibile monitorare i progressi nella pagina Audit.

Se riscontri problemi durante la distribuzione del sistema Cloud Volumes ONTAP , rivedi il messaggio di errore. È anche possibile selezionare il sistema e fare clic su **Ricrea ambiente**.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

> Una volta completato il processo di distribuzione, non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale di Azure, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdite di dati.

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Avvia una coppia Cloud Volumes ONTAP HA in Azure

Se si desidera avviare una coppia Cloud Volumes ONTAP HA in Azure, è necessario creare un sistema HA nella console.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire le istruzioni.
3. Se richiesto, "creare un agente Console" .
4. **Dettagli e credenziali**: facoltativamente, modifica le credenziali e la sottoscrizione di Azure, specifica un nome per il cluster, aggiungi tag se necessario e quindi specifica le credenziali.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia la macchina virtuale di Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.
Tag del gruppo di risorse	I tag sono metadati per le risorse di Azure. Quando si immettono tag in questo campo, la Console li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP . Quando si crea un sistema, è possibile aggiungere fino a quattro tag dall'interfaccia utente, per poi aggiungerne altri dopo la creazione. Tieni presente che l'API non ti limita a quattro tag quando crei un sistema. Per informazioni sui tag, fare riferimento a "Documentazione di Microsoft Azure: utilizzo dei tag per organizzare le risorse di Azure" .
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.

Campo	Descrizione
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP . Per distribuire un sistema Cloud Volumes ONTAP con pagamento in base al consumo, è necessario associare una sottoscrizione di Azure Marketplace alla sottoscrizione di Azure selezionata. "Scopri come aggiungere le credenziali" .

5. **Servizi**: abilita o disabilita i singoli servizi a seconda che tu voglia utilizzarli con Cloud Volumes ONTAP.
   - "Scopri di più sulla NetApp Data Classification"
   - "Scopri di più su NetApp Backup and Recovery"

   Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

6. **Modelli di distribuzione HA**:
   a. Selezionare **Zona di disponibilità singola** o **Zona di disponibilità multipla**.
      - Per singole zone di disponibilità, selezionare un'area di Azure, una zona di disponibilità, una rete virtuale e una subnet.

        A partire da Cloud Volumes ONTAP 9.15.1, è possibile distribuire istanze di macchine virtuali (VM) in modalità HA in singole zone di disponibilità (AZ) in Azure. È necessario selezionare una zona e una regione che supportino questa distribuzione. Se la zona o la regione non supporta la distribuzione zonale, viene seguita la precedente modalità di distribuzione non zonale per LRS. Per comprendere le configurazioni supportate per i dischi gestiti condivisi, fare riferimento a"Configurazione della zona di disponibilità singola HA con dischi gestiti condivisi" .

      - Per più zone di disponibilità, selezionare una regione, una rete virtuale, una subnet, una zona per il nodo 1 e una zona per il nodo 2.

   b. Seleziona la casella di controllo **Ho verificato la connettività di rete…**.
7. **Connettività**: scegli un gruppo di risorse nuovo o esistente e poi scegli se utilizzare il gruppo di sicurezza predefinito o il tuo.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Gruppo di risorse	Crea un nuovo gruppo di risorse per Cloud Volumes ONTAP oppure utilizza un gruppo di risorse esistente. La procedura consigliata è quella di utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile distribuire Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, questa operazione non è consigliata a causa del rischio di perdita di dati. Per maggiori dettagli, vedere l'avviso sopra. È necessario utilizzare un gruppo di risorse dedicato per ogni coppia Cloud Volumes ONTAP HA distribuita in Azure. In un gruppo di risorse è supportata solo una coppia HA. La console riscontra problemi di connessione se si tenta di distribuire una seconda coppia Cloud Volumes ONTAP HA in un gruppo di risorse di Azure. Se l'account Azure che stai utilizzando ha il "permessi richiesti" , la Console rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di distribuzione o eliminazione.
Gruppo di sicurezza generato	Se lasci che sia la Console a generare il gruppo di sicurezza per te, devi scegliere come consentire il traffico: • Se si sceglie **Solo VNet selezionata**, l'origine del traffico in entrata è l'intervallo di subnet della VNet selezionata e l'intervallo di subnet della VNet in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le reti virtuali**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizzare esistente	Se si sceglie un gruppo di sicurezza esistente, questo deve soddisfare i requisiti di Cloud Volumes ONTAP . "Visualizza il gruppo di sicurezza predefinito" .

8. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp .
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP" .
   - "Scopri come impostare le licenze" .
9. **Pacchetti preconfigurati**: seleziona uno dei pacchetti per distribuire rapidamente un sistema Cloud Volumes ONTAP oppure fai clic su **Modifica configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.
10. **Licenze**: modifica la versione di Cloud Volumes ONTAP in base alle tue esigenze e seleziona un tipo di macchina virtuale.

    Se per la versione selezionata è disponibile una versione Release Candidate, una versione General Availability o una patch più recente, la Console aggiorna il sistema a tale versione durante la sua creazione. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.13.1 e se è disponibile la versione 9.13.1 P4. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.13 alla 9.14.

11. **Iscriviti da Azure Marketplace**: segui i passaggi se la console non riesce ad abilitare le distribuzioni programmatiche di Cloud Volumes ONTAP.
12. **Risorse di archiviazione sottostanti**: scegli le impostazioni per l'aggregato iniziale: un tipo di disco, una dimensione per ciascun disco e se abilitare la suddivisione dei dati in livelli nell'archiviazione BLOB.

    Notare quanto segue:

    - La dimensione del disco si riferisce a tutti i dischi nell'aggregato iniziale e a tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.

      Per assistenza nella scelta della dimensione del disco, fare riferimento a"Dimensiona il tuo sistema in Azure" .

    - Se l'accesso pubblico al tuo account di archiviazione è disabilitato all'interno della VNet, non puoi abilitare la suddivisione in livelli dei dati nel tuo sistema Cloud Volumes ONTAP . Per informazioni, fare riferimento a"Regole del gruppo di sicurezza" .
    - Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
    - Se si disabilita la suddivisione in livelli dei dati, è possibile abilitarla sugli aggregati successivi.

      "Scopri di più sulla suddivisione in livelli dei dati" .

    - A partire da Cloud Volumes ONTAP 9.15.0P1, i BLOB di pagine di Azure non sono più supportati per le nuove distribuzioni di coppie ad alta disponibilità. Se attualmente si utilizzano BLOB di pagine di Azure in distribuzioni di coppie ad alta disponibilità esistenti, è possibile eseguire la migrazione a tipi di istanze di VM più recenti nelle VM della serie Edsv4 e nelle VM della serie Edsv5.

      "Scopri di più sulle configurazioni supportate in Azure" .

13. **Velocità di scrittura e WORM**:

    a. Se lo desideri, seleziona la velocità di scrittura **Normale** o **Alta**.

       "Scopri di più sulla velocità di scrittura" .

    b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

       Questa opzione è disponibile solo per alcuni tipi di VM. Per scoprire quali tipi di VM sono supportati, fare riferimento a"Configurazioni supportate per licenza per coppie HA" .

       WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

    "Scopri di più sullo storage WORM" .

    a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.
14. **Comunicazione sicura con Storage e WORM**: scegli se abilitare una connessione HTTPS agli account di storage di Azure e attivare lo storage WORM (Write Once, Read Many), se lo desideri.

    La connessione HTTPS avviene da una coppia Cloud Volumes ONTAP 9.7 HA agli account di archiviazione BLOB di pagine di Azure. Tieni presente che l'abilitazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato il sistema.

"Scopri di più sullo storage WORM" .

WORM non può essere abilitato se è stato abilitato il tiering dei dati.

"Scopri di più sullo storage WORM" .

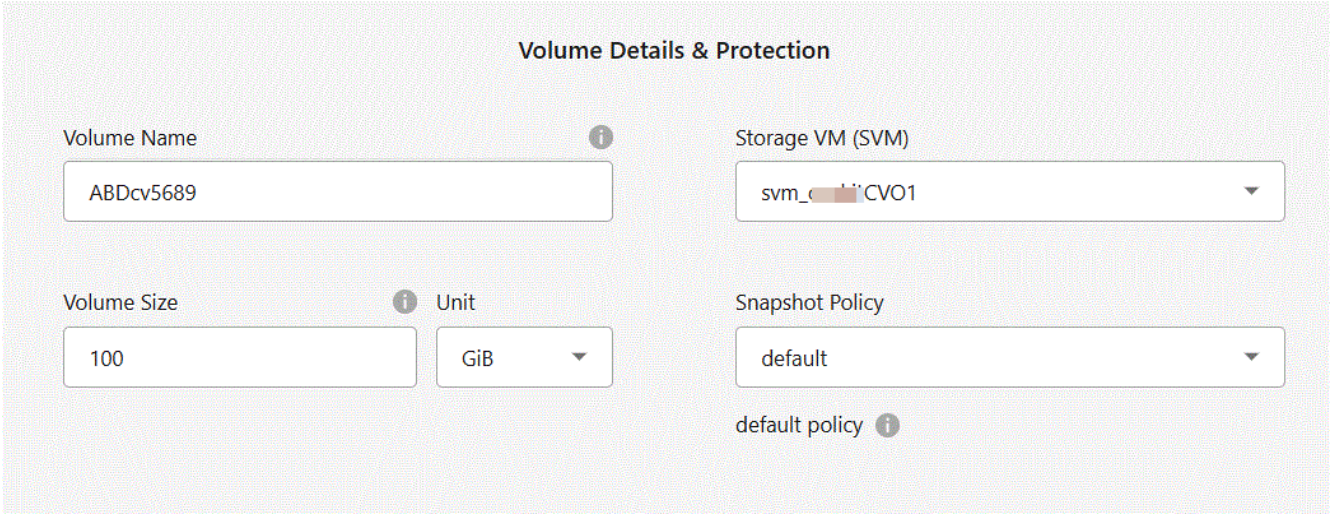
15. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

    "Scopri i protocolli e le versioni client supportati" .

    Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

    L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



16. **Configurazione CIFS**: se hai scelto il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Per configurare Azure AD Domain Services come server AD per Cloud Volumes ONTAP, è necessario immettere **OU=Computer AADDC** o **OU=Utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: creare un'unità organizzativa (OU) in un dominio gestito da Azure AD Domain Services"^]
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

17. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Scegli un profilo di utilizzo del volume" ,"Panoramica della

suddivisione in livelli dei dati" , E "KB: Quali funzionalità di Inline Storage Efficiency sono supportate da CVO?"

18. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fare clic su **Ulteriori informazioni** per esaminare i dettagli sul supporto e sulle risorse di Azure che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console distribuisce il sistema Cloud Volumes ONTAP . È possibile monitorare i progressi nella pagina Audit.

Se riscontri problemi durante la distribuzione del sistema Cloud Volumes ONTAP , rivedi il messaggio di errore. È anche possibile selezionare il sistema e fare clic su **Ricrea ambiente**.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

> Una volta completato il processo di distribuzione, non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale di Azure, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdite di dati.

Link correlati

*"Pianificazione della configurazione Cloud Volumes ONTAP in Azure" *"Distribuisci Cloud Volumes ONTAP in Azure da Azure Marketplace"

Verifica l'immagine della piattaforma Azure

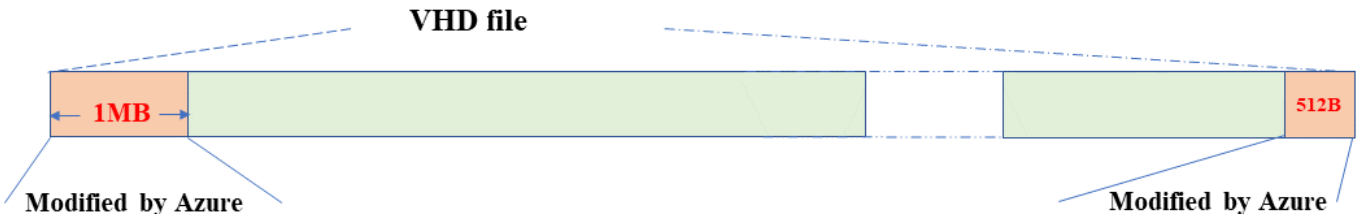
Verifica delle immagini di Azure Marketplace per Cloud Volumes ONTAP

La verifica delle immagini di Azure è conforme ai requisiti di sicurezza avanzati NetApp . La verifica di un file immagine è un processo semplice. Tuttavia, la verifica della firma dell'immagine di Azure richiede considerazioni specifiche per il file immagine VHD di Azure, poiché viene modificato in Azure Marketplace.

> La verifica delle immagini di Azure è supportata su Cloud Volumes ONTAP 9.15.0 e versioni successive.

Alterazione dei file VHD pubblicati da parte di Azure

1 MB (1048576 byte) all'inizio e 512 byte alla fine del file VHD vengono modificati da Azure. NetApp firma il file VHD rimanente.



Nell'esempio, il file VHD è di 10 GB. La parte firmata NetApp è contrassegnata in verde (10 GB - 1 MB - 512 byte).

Link correlati

- "Blog Page Fault: come firmare e verificare utilizzando OpenSSL"
- "Utilizzare l'immagine di Azure Marketplace per creare un'immagine di macchina virtuale per la GPU di Azure Stack Edge Pro | Microsoft Learn"
- "Esportare/copiare un disco gestito in un account di archiviazione tramite l'interfaccia della riga di comando di Azure | Microsoft Learn"
- "Guida introduttiva ad Azure Cloud Shell - Bash | Microsoft Learn"
- "Come installare l'interfaccia della riga di comando di Azure | Microsoft Learn"
- "copia blob di archiviazione az | Microsoft Learn"
- "Sign in con Azure CLI — Accesso e autenticazione | Microsoft Learn"

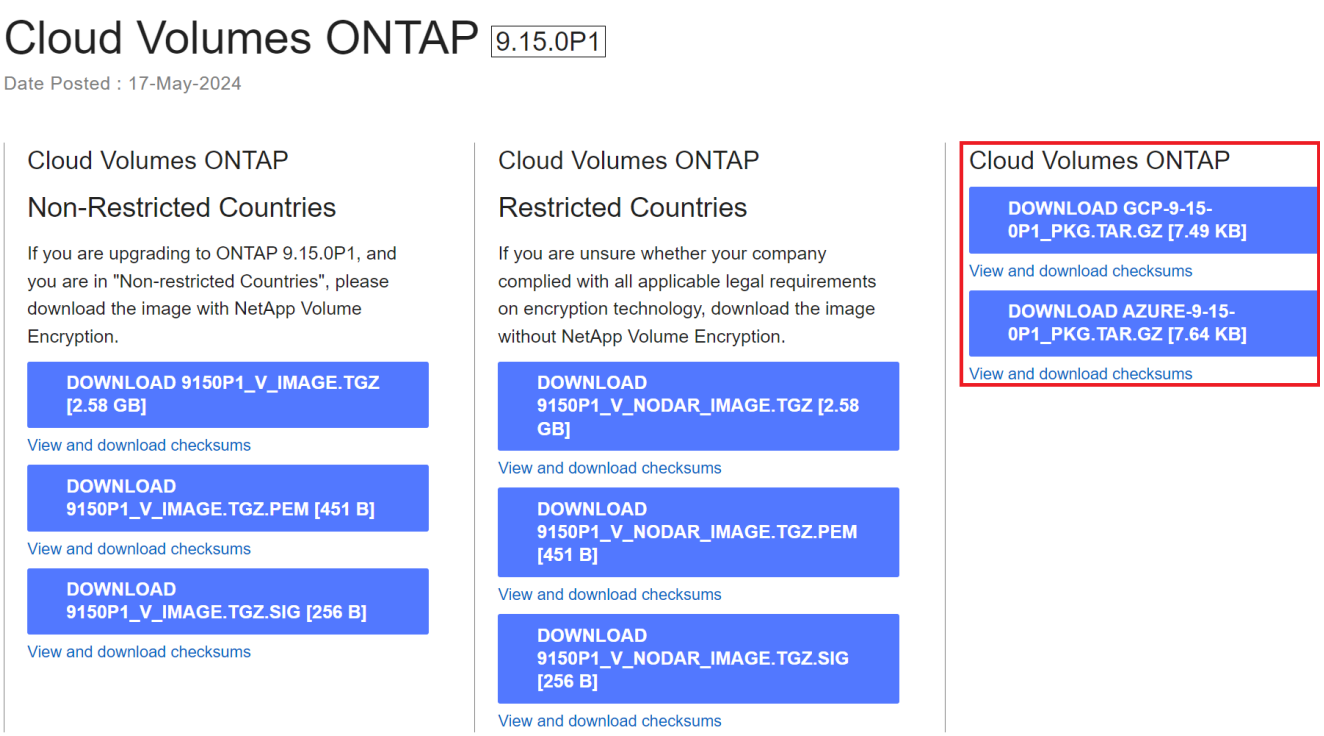
Scarica il file immagine di Azure per Cloud Volumes ONTAP

È possibile scaricare il file immagine di Azure da "Sito di supporto NetApp" .

Il file *tar.gz* contiene i file necessari per la verifica della firma dell'immagine. Insieme al file *tar.gz*, dovresti scaricare anche il file *checksum* per l'immagine. Il file di checksum contiene il `md5` E `sha256` checksum del file *tar.gz*.

Passi

1. Vai al "Pagina del prodotto Cloud Volumes ONTAP sul sito di supporto NetApp" e scaricare la versione software richiesta dalla sezione **Download**.
2. Nella pagina di download Cloud Volumes ONTAP , fare clic sul file scaricabile per l'immagine di Azure e scaricare il file *tar.gz*.



3. Su Linux, esegui `md5sum AZURE-<version>_PKG.TAR.GZ` .

   Su macOS, esegui `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Verificare che il `md5sum` E `sha256sum` i valori corrispondono a quelli nell'immagine di Azure scaricata.
5. Su Linux e macOS, estrarre il file *tar.gz* utilizzando `tar -xzf` comando.

   Il file *tar.gz* estratto contiene il file digest (*.sig*), il file del certificato della chiave pubblica (*.pem*) e il file del certificato della catena (*.pem*).

   Esempio di output dopo l'estrazione del file tar.gz:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Esportare immagini VHD per Cloud Volumes ONTAP da Azure Marketplace

Una volta pubblicata sul cloud di Azure, l'immagine VHD non è più gestita da NetApp. L'immagine pubblicata viene invece inserita nel marketplace di Azure. Quando l'immagine viene preparata e pubblicata su Azure Marketplace, Azure modifica 1 MB all'inizio e 512 byte alla fine del VHD. Per verificare la firma del file VHD, è necessario esportare l'immagine VHD modificata da Azure da Azure Marketplace.

Prima di iniziare

Assicurati che l'interfaccia della riga di comando di Azure sia installata sul tuo sistema oppure che Azure Cloud Shell sia disponibile tramite il portale di Azure. Per ulteriori informazioni su come installare l'interfaccia della riga di comando di Azure, fare riferimento a "Documentazione Microsoft: come installare l'interfaccia della riga di comando di Azure" .

Passi

1. Mappare la versione Cloud Volumes ONTAP sul sistema alla versione dell'immagine di Azure Marketplace utilizzando il contenuto del file *version_readme*. La versione Cloud Volumes ONTAP è rappresentata da `buildname` e la versione dell'immagine di Azure Marketplace è rappresentata da `version` nelle mappature delle versioni.

   Nell'esempio seguente, la versione Cloud Volumes ONTAP `9.15.0P1` è mappato alla versione dell'immagine di Azure Marketplace `9150.01000024.05090105` . Questa versione dell'immagine di Azure Marketplace viene utilizzata in seguito per impostare l'URN dell'immagine.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identifica la regione in cui desideri creare le VM. Il nome della regione viene utilizzato come valore per `locName` variabile quando si imposta l'URN dell'immagine del marketplace. Per elencare le regioni disponibili, eseguire questo comando:

   ```
   az account list-locations -o table
   ```

   In questa tabella, il nome della regione appare nella `Name` campo.

   ```
   $ az account list-locations -o table
   DisplayName               Name                 RegionalDisplayName
   ------------------------  -------------------
   ------------------------------------
   East US                   eastus               (US) East US
   East US 2                 eastus2              (US) East US 2
   South Central US          southcentralus       (US) South Central US
   ...
   ```

3. Esaminare i nomi SKU per le versioni Cloud Volumes ONTAP corrispondenti e i tipi di distribuzione delle VM nella tabella seguente. Il nome SKU viene utilizzato come valore per `skuName` variabile quando si imposta l'URN dell'immagine del marketplace.

   Ad esempio, tutte le distribuzioni a nodo singolo con Cloud Volumes ONTAP 9.15.0 dovrebbero utilizzare `ontap_cloud_byol` come nome SKU.

* Versione Cloud Volumes ONTAP *	**Distribuzione VM tramite**	**Nome SKU**
9.17.1 e versioni successive	Il marketplace di Azure	ontap_cloud_direct_gen2
9.17.1 e versioni successive	La NetApp Console	ontap_cloud_gen2
9.16.1	Il marketplace di Azure	ontap_cloud_direct
9.16.1	La console	ontap_cloud
9.15.1	La console	ontap_cloud
9.15.0	La console, distribuzioni a nodo singolo	ontap_cloud_byol
9.15.0	La console, distribuzioni ad alta disponibilità (HA)	ontap_cloud_byol_ha

4. Dopo aver mappato la versione ONTAP e l'immagine di Azure Marketplace, esportare il file VHD da Azure Marketplace utilizzando Azure Cloud Shell o Azure CLI.

Esportare file VHD utilizzando Azure Cloud Shell su Linux

Da Azure Cloud Shell, esporta l'immagine del marketplace nel file VHD (ad esempio, *9150.01000024.05090105.vhd*) e scaricala sul tuo sistema Linux locale. Per ottenere l'immagine VHD da Azure Marketplace, eseguire i passaggi seguenti.

Passi

1. Imposta l'URN e altri parametri dell'immagine del marketplace. Il formato URN è `<publisher>:<offer>:<sku>:<version>` . Facoltativamente, puoi elencare le immagini del marketplace NetApp per confermare la versione corretta dell'immagine.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Crea un nuovo disco gestito dall'immagine del marketplace con la versione dell'immagine corrispondente:

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Esportare il file VHD dal disco gestito ad Azure Storage. Creare un contenitore con il livello di accesso appropriato. In questo esempio, abbiamo utilizzato un contenitore denominato `vm-images` con `Container` livello di accesso. Ottieni la chiave di accesso dell’account di archiviazione dal portale di Azure: **Account di archiviazione > *examplesaname* > Chiave di accesso > *key1* > *key* > Mostra > *<copia>***

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Scarica l’immagine generata sul tuo sistema Linux. Utilizzare il `wget` comando per scaricare il file VHD:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

L’URL segue un formato standard. Per l’automazione, è possibile ricavare la stringa URL come mostrato di seguito. In alternativa, puoi usare l’interfaccia della riga di comando di Azure `az` comando per ottenere l’URL. Esempio di URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Pulisci il disco gestito

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Esportare il file VHD utilizzando l'interfaccia della riga di comando di Azure su Linux

Esportare l'immagine del marketplace in un file VHD tramite l'interfaccia della riga di comando di Azure da un sistema Linux locale.

Passi

1. Accedi all'interfaccia della riga di comando di Azure ed elenca le immagini del marketplace:

```
% az login --use-device-code
```

2. Per accedere, utilizzare un browser Web per aprire la pagina https://microsoft.com/devicelogin e inserisci il codice di autenticazione.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Crea un nuovo disco gestito dall'immagine del marketplace con la versione dell'immagine corrispondente.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

Per automatizzare il processo, è necessario estrarre il SAS dall'output standard. Per indicazioni fare riferimento ai documenti appropriati.

4. Esportare il file VHD dal disco gestito.

   a. Creare un contenitore con il livello di accesso appropriato. In questo esempio, un contenitore denominato `vm-images` con `Container` viene utilizzato il livello di accesso.

   b. Ottieni la chiave di accesso dell'account di archiviazione dal portale di Azure: **Account di archiviazione > *examplesaname* > Chiave di accesso > *key1* > *key* > Mostra > <*copia*>**

      Puoi anche usare il `az` comando per questo passaggio.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Controllare lo stato della copia del blob.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Scarica l'immagine generata sul tuo server Linux.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

L'URL segue un formato standard. Per l'automazione, è possibile ricavare la stringa URL come mostrato di seguito. In alternativa, puoi usare l'interfaccia della riga di comando di Azure `az` comando per ottenere l'URL. Esempio di URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Pulisci il disco gestito

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

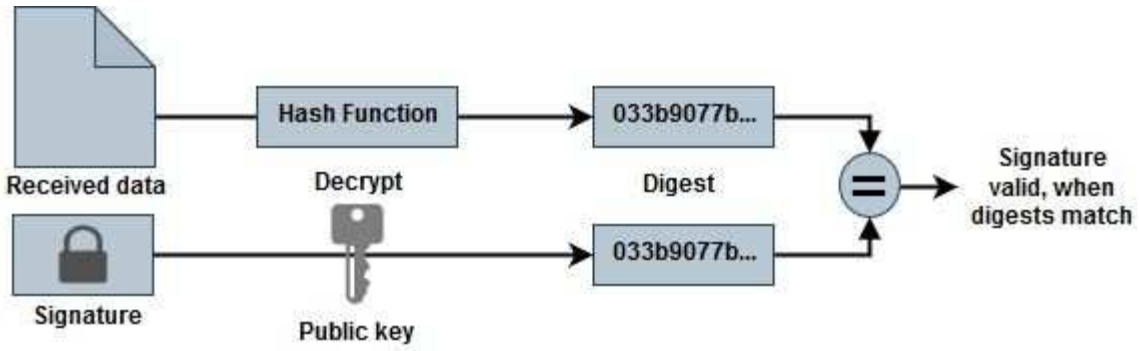
Verifica la firma del file

Verifica della firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP

Il processo di verifica dell'immagine di Azure genera un file digest dal file VHD eliminando 1 MB all'inizio e 512 byte alla fine, quindi applicando una funzione hash. Per abbinare la procedura di firma, per l'hashing viene utilizzato *sha256*.

Riepilogo del flusso di lavoro di verifica della firma del file

Di seguito è riportata una panoramica del processo di verifica della firma del file.



- Scaricamento dell'immagine di Azure da "Sito di supporto NetApp" ed estraendo il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem). Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.
- Verifica della catena di fiducia.
- Estrazione della chiave pubblica (.pub) dal certificato della chiave pubblica (.pem).
- Decifrare il file digest utilizzando la chiave pubblica estratta.
- Confronto del risultato con un digest appena generato di un file temporaneo creato dal file immagine dopo aver rimosso 1 MB all'inizio e 512 byte alla fine. Questo passaggio viene eseguito utilizzando lo strumento da riga di comando OpenSSL. Lo strumento OpenSSL CLI visualizza un messaggio appropriato in caso di successo o fallimento nella corrispondenza dei file.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su Linux

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Passi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.

2. Verificare la catena di fiducia.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica.

   Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Pulisci l'area di lavoro.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su macOS

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Passi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.

2. Verificare la catena di fiducia.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `tail -c` . Tieni presente

che su macOS il comando tail potrebbe richiedere circa dieci minuti per essere completato.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica. Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Pulisci l'area di lavoro.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Distribuisci Cloud Volumes ONTAP dal marketplace di Azure

È possibile utilizzare la distribuzione diretta di Azure Marketplace per distribuire Cloud Volumes ONTAP in modo rapido e semplice. Dall'Azure Marketplace puoi distribuire rapidamente Cloud Volumes ONTAP in pochi clic ed esplorare le sue funzionalità e capacità principali nel tuo ambiente.

Per maggiori informazioni su questa offerta, fare riferimento a"Scopri di più sulle offerte Cloud Volumes ONTAP nella NetApp Console e nel marketplace" .

Informazioni su questo compito

Il sistema Cloud Volumes ONTAP distribuito tramite la distribuzione diretta di Azure Marketplace presenta le seguenti proprietà. Si noti che le funzionalità di un'istanza autonoma distribuita tramite Azure Marketplace cambiano quando viene rilevata nella NetApp Console.

- L'ultima versione Cloud Volumes ONTAP (9.16.1 o successiva).
- Una licenza gratuita per Cloud Volumes ONTAP limitata a 500 GiB di capacità fornita. Questa licenza non include alcun supporto NetApp e non ha una data di scadenza.

- Due nodi configurati in modalità ad alta disponibilità (HA) in un'unica zona di disponibilità (AZ), dotati di numeri di serie predefiniti. Le macchine virtuali di storage (VM di storage) vengono distribuite in un"modalità di orchestrazione flessibile" .
- Un aggregato per l'istanza creata per impostazione predefinita.
- Un disco gestito Premium SSD v2 con capacità di provisioning di 500 GiB, un disco root e un disco dati.
- Una VM di archiviazione dati distribuita, con servizi dati NFS, CIFS, iSCSI e NVMe/TCP. Non è possibile aggiungere ulteriori VM di archiviazione dati.
- Licenze installate per NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock e SnapMirror.
- "Efficienza di stoccaggio sensibile alla temperatura (TSSE) ONTAP", crittografia del volume e gestione delle chiavi esterne abilitate per impostazione predefinita.
- Queste funzionalità non sono supportate:
  - Struttura a FabricPool
  - Modifica del tipo di VM di archiviazione
  - Modalità di scrittura veloce

Prima di iniziare

- Assicurati di disporre di un abbonamento valido ad Azure Marketplace.
- Assicurati di soddisfare i requisiti di rete per un"Distribuzione HA in una singola AZ" in Azzurro. Fare riferimento a "Configurare la rete di Azure per Cloud Volumes ONTAP" .
- Per distribuire Cloud Volumes ONTAP è necessario che ti venga assegnato uno di questi ruoli di Azure:
  - IL `contributor` ruolo con le autorizzazioni predefinite. Per maggiori informazioni, fare riferimento al "Documentazione di Microsoft Azure: ruoli predefiniti di Azure" .
  - Un ruolo RBAC personalizzato con le seguenti autorizzazioni. Per maggiori informazioni, fare riferimento al "Documentazione di Azure: ruoli personalizzati di Azure" .

```
"autorizzazioni": [ { "azioni": [ "Microsoft.AAD/register/azione",
"Microsoft.Resources/sottoscrizioni/GruppiDiRisorse/scrittura",
"Microsoft.Network/loadBalancers/scrittura", "Microsoft.ClassicCompute/Machines
virtuali/scrittura", "Microsoft.Compute/capacityReservationGroups/distribuzione/azione",
"Microsoft.ClassicCompute/Machines
virtuali/Interfacciadirete/associataGruppiDiSecurità/scrittura",
"Microsoft.Network/Interfacciadirete/scrittura", "Microsoft.Compute/Machines virtuali/scrittura",
"Microsoft.Compute/Machines virtuali/estensioni/scrittura",
"Microsoft.Resources/distribuzioni/validazione/azione",
"Microsoft.Resources/sottoscrizioni/GruppiDiRisorse/lettura",
"Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```

Se hai registrato il provider di risorse "Microsoft.storage" nel tuo abbonamento, non hai bisogno di `Microsoft.AAD/register/action` permesso. Per maggiori informazioni, fare riferimento al "Documentazione di Azure: autorizzazioni di Azure per l'archiviazione" .

Passi

1. Dal sito di Azure Marketplace, cerca i prodotti NetApp .
2. Selezionare * NetApp Cloud Volumes ONTAP diretto*.
3. Fare clic su **Crea** per avviare la procedura guidata di distribuzione.
4. Seleziona un piano. L'elenco **Piano** in genere visualizza le versioni più recenti di Cloud Volumes ONTAP.
5. Nella scheda **Informazioni di base**, fornisci questi dettagli:
   - **Abbonamento**: Seleziona un abbonamento. L'implementazione sarà collegata al numero di abbonamento.
   - **Gruppo di risorse**: utilizza un gruppo di risorse esistente o creane uno nuovo. I gruppi di risorse aiutano ad allocare tutte le risorse, come dischi e VM di archiviazione, all'interno di un singolo gruppo per un sistema Cloud Volumes ONTAP .
   - **Regione**: seleziona una regione che supporti la distribuzione di Azure HA in una singola zona di disponibilità. Nell'elenco vengono visualizzate solo le regioni disponibili.
   - **Dimensione**: seleziona una dimensione di archiviazione VM per il disco gestito Premium SSD v2 supportato.
   - **Zona**: seleziona una zona per la regione selezionata.
   - **Password amministratore**: imposta una password. Questa password di amministratore verrà utilizzata per accedere al sistema dopo la distribuzione.
   - **Conferma password**: reinserisci la stessa password per conferma.
     - Nella scheda **Rete**, aggiungi una rete virtuale e una subnet oppure selezionale dagli elenchi.

       Per rispettare le restrizioni di Microsoft Azure, è necessario creare una nuova subnet quando si configura una nuova rete virtuale. Allo stesso modo, se si sceglie una rete esistente, è necessario selezionare una subnet esistente.

     - Per selezionare un gruppo di sicurezza di rete predefinito, selezionare **Sì**. Selezionare **No** per assegnare un gruppo di sicurezza di rete di Azure predefinito con le regole di traffico necessarie. Per ulteriori informazioni, fare riferimento a "Regole del gruppo di sicurezza per Azure" .
     - Nella scheda **Avanzate** verificare se sono state impostate le due funzionalità di Azure necessarie per questa distribuzione. Fare riferimento a"Abilita una funzionalità di Azure per le distribuzioni AZ singole Cloud Volumes ONTAP" E"Abilita la modalità ad alta disponibilità per Cloud Volumes ONTAP in Azure" .
     - Nella scheda **Tag** è possibile definire coppie nome-valore per le risorse o i gruppi di risorse.
     - Nella scheda **Revisiona + crea**, rivedi i dettagli e avvia la distribuzione.

Dopo aver finito

Seleziona l'icona di notifica per visualizzare lo stato di avanzamento della distribuzione. Dopo aver distribuito Cloud Volumes ONTAP , è possibile visualizzare la VM di archiviazione elencata per le operazioni.

Una volta accessibile, utilizzare ONTAP System Manager o ONTAP CLI per accedere alla VM di archiviazione

con le credenziali di amministratore impostate. Successivamente, è possibile creare volumi, LUN o condivisioni e iniziare a utilizzare le capacità di archiviazione di Cloud Volumes ONTAP.

Risolvere i problemi di distribuzione

I sistemi Cloud Volumes ONTAP distribuiti direttamente tramite Azure Marketplace non includono il supporto di NetApp. Se durante la distribuzione si verificano problemi, è possibile risolverli in modo indipendente.

Passi

1. Nel sito di Azure Marketplace, vai a **Diagnostica di avvio > Registro seriale**.
2. Scaricare ed esaminare i registri seriali.
3. Per la risoluzione dei problemi, consultare la documentazione del prodotto e gli articoli della knowledge base (KB).
   - "Documentazione di Azure Marketplace"
   - "Documentazione NetApp"
   - "Articoli della Knowledge Base NetApp"

Scopri i sistemi distribuiti nella Console

È possibile individuare i sistemi Cloud Volumes ONTAP distribuiti tramite la distribuzione diretta di Azure Marketplace e gestirli nella pagina **Sistemi** nella Console. L'agente Console rileva i sistemi, li aggiunge e applica le licenze necessarie, sbloccando così tutte le funzionalità della Console per questi sistemi. La configurazione HA originale in una singola AZ con dischi gestiti PSSD v2 viene mantenuta e il sistema viene registrato nella stessa sottoscrizione Azure e nello stesso gruppo di risorse della distribuzione originale.

Informazioni su questo compito

Dopo aver individuato i sistemi Cloud Volumes ONTAP distribuiti tramite la distribuzione diretta di Azure Marketplace, l'agente della console esegue queste attività:

- Sostituisce le licenze gratuite dei sistemi scoperti come normali licenze basate sulla capacità"Licenze Freemium" .
- Mantiene le funzionalità esistenti dei sistemi distribuiti e aggiunge le funzionalità aggiuntive della Console, come la protezione dei dati, la gestione dei dati e le funzionalità di sicurezza.
- Sostituisce le licenze installate sui nodi con nuove licenze ONTAP per NFS, CIFS (SMB), iSCSI, ARP, SnapLock e SnapMirror.
- Converte i numeri di serie dei nodi generici in numeri di serie univoci.
- Assegna nuovi tag di sistema alle risorse secondo necessità.
- Converte gli indirizzi IP dinamici dell'istanza in indirizzi IP statici.
- Abilita le funzionalità di"Struttura a FabricPool" ,"AutoSupport" , E"scrivi una volta, leggi molte volte" (WORM) di archiviazione sui sistemi distribuiti. Puoi attivare queste funzionalità dalla Console quando ne hai bisogno.
- Registra le istanze negli account NSS utilizzati per individuarle.
- Abilita le funzionalità di gestione della capacità in"modalità automatica e manuale" per i sistemi scoperti.

Prima di iniziare

Assicurarsi che la distribuzione sia completa su Azure Marketplace. L'agente della console può rilevare i sistemi solo quando la distribuzione è completa e sono disponibili per la rilevazione.

Passi

Nella Console, segui la procedura standard per rilevare i sistemi esistenti. Fare riferimento a "Aggiungere un sistema Cloud Volumes ONTAP esistente alla console" .

> Durante l'individuazione, potrebbero essere visualizzati messaggi di errore, ma è possibile ignorarli finché il processo di individuazione non sarà completato. Non modificare le configurazioni Cloud Volumes ONTAP generate dal sistema nel portale di Azure Marketplace durante l'individuazione, in particolare i tag di sistema. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti del sistema.

Dopo aver finito

Una volta completata l'individuazione, è possibile visualizzare i sistemi elencati nella pagina **Sistemi** nella Console. È possibile eseguire varie attività di gestione, come ad esempio"espandendo l'aggregato" ,"aggiunta di volumi" ,"provisioning di VM di storage aggiuntive" , E"modifica dei tipi di istanza" .

Link correlati

Per ulteriori informazioni sulla creazione di storage, fare riferimento alla documentazione ONTAP :

- "Creare volumi per NFS"
- "Creare LUN per iSCSI"
- "Crea azioni per CIFS"

Inizia a usare Google Cloud

Avvio rapido per Cloud Volumes ONTAP in Google Cloud

Inizia a usare Cloud Volumes ONTAP in Google Cloud in pochi passaggi.

Creare un agente Console

Se non hai un "Agente console" eppure devi crearne uno. "Scopri come creare un agente Console in Google Cloud"

Tieni presente che se desideri distribuire Cloud Volumes ONTAP in una subnet in cui non è disponibile l'accesso a Internet, dovrai installare manualmente l'agente Console e accedere alla NetApp Console in esecuzione su tale agente Console. "Scopri come installare manualmente l'agente Console in una posizione senza accesso a Internet"

Pianifica la tua configurazione

La Console offre pacchetti preconfigurati che soddisfano i requisiti del tuo carico di lavoro, oppure puoi creare la tua configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione.

"Scopri di più sulla pianificazione della tua configurazione" .

Configura la tua rete

1. Assicurati che la tua VPC e le tue subnet supportino la connettività tra l'agente della console e Cloud Volumes ONTAP.
2. Se si prevede di abilitare la suddivisione in livelli dei dati, "configurare la subnet Cloud Volumes ONTAP per l'accesso privato a Google" .
3. Se si distribuisce una coppia HA, assicurarsi di disporre di quattro VPC, ciascuna con la propria subnet.
4. Se si utilizza una VPC condivisa, fornire il ruolo *Compute Network User* all'account del servizio agente della console.
5. Abilita l'accesso a Internet in uscita dalla VPC di destinazione per NetApp AutoSupport.

   Questo passaggio non è necessario se si distribuisce Cloud Volumes ONTAP in una posizione in cui non è disponibile l'accesso a Internet.

"Scopri di più sui requisiti di rete" .

Configurare un account di servizio

Cloud Volumes ONTAP richiede un account di servizio Google Cloud per due scopi. Il primo è quando abiliti"livelli di dati" per suddividere i dati inutilizzati in un archivio di oggetti a basso costo su Google Cloud. Il secondo è quando si abilita il "NetApp Backup and Recovery" per eseguire il backup di volumi su storage di oggetti a basso costo.

È possibile configurare un account di servizio e utilizzarlo per entrambi gli scopi. L'account di servizio deve avere il ruolo **Amministratore archiviazione**.

"Leggi le istruzioni passo passo" .

Abilita le API di Google Cloud

"Abilita le API di Google Cloud nel tuo progetto". "Queste API", che potresti aver già abilitato durante la creazione dell'agente Console, sono necessari per distribuire Cloud Volumes ONTAP in Google Cloud.

Avvia Cloud Volumes ONTAP tramite la console

Fare clic su **Aggiungi sistema**, selezionare il tipo di sistema che si desidera distribuire e completare i passaggi della procedura guidata. "Leggi le istruzioni passo passo" .

Link correlati

- "Creazione di un agente Console"
- "Installazione del software dell'agente Console su un host Linux"
- "Autorizzazioni di Google Cloud per l'agente della console"

Pianifica la configurazione Cloud Volumes ONTAP in Google Cloud

Quando distribuisci Cloud Volumes ONTAP in Google Cloud, puoi scegliere un sistema preconfigurato che soddisfi i requisiti del tuo carico di lavoro oppure puoi creare una configurazione personalizzata. Se scegli una configurazione personalizzata, dovresti conoscere le opzioni a tua disposizione.

Scegli una licenza Cloud Volumes ONTAP

Sono disponibili diverse opzioni di licenza per Cloud Volumes ONTAP. Ogni opzione ti consente di scegliere il modello di consumo più adatto alle tue esigenze.

- "Scopri le opzioni di licenza per Cloud Volumes ONTAP"
- "Scopri come impostare le licenze"

Scegli una regione supportata

Cloud Volumes ONTAP è supportato nella maggior parte delle regioni Google Cloud. "Visualizza l'elenco completo delle regioni supportate" .

Scegli un tipo di macchina supportato

Cloud Volumes ONTAP supporta diversi tipi di macchine, a seconda del tipo di licenza scelto.

"Configurazioni supportate per Cloud Volumes ONTAP in Google Cloud"

Comprendere i limiti di archiviazione

Il limite di capacità raw per un sistema Cloud Volumes ONTAP è legato alla licenza. Ulteriori limiti incidono sulle dimensioni degli aggregati e sui volumi. Quando pianifichi la tua configurazione, dovresti essere consapevole di questi limiti.

"Limiti di storage per Cloud Volumes ONTAP in Google Cloud"

Dimensiona il tuo sistema in Google Cloud

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di prestazioni e capacità. Quando si sceglie un tipo di macchina, un tipo di disco e una dimensione del disco, è necessario tenere presenti alcuni punti chiave:

Tipo di macchina

Guarda i tipi di macchina supportati in "Note sulla versione Cloud Volumes ONTAP" e poi rivedere i dettagli di Google su ciascun tipo di macchina supportato. Adatta i requisiti del carico di lavoro al numero di vCPU e di memoria per il tipo di macchina. Si noti che ogni core della CPU aumenta le prestazioni di rete.

Per maggiori dettagli fare riferimento a quanto segue:

- "Documentazione di Google Cloud: tipi di macchine standard N1"
- "Documentazione di Google Cloud: Prestazioni"

Tipi di disco

Quando si creano volumi per Cloud Volumes ONTAP, è necessario scegliere lo storage cloud sottostante che Cloud Volumes ONTAP utilizza per un disco. Il tipo di disco può essere uno dei seguenti:

- *Dischi persistenti SSD zonali*: i dischi persistenti SSD sono ideali per carichi di lavoro che richiedono elevati tassi di IOPS casuali.
- *Dischi persistenti bilanciati zonali*: questi SSD bilanciano prestazioni e costi offrendo IOPS inferiori per GB.
- *Dischi persistenti standard zonali*: i dischi persistenti standard sono economici e possono gestire operazioni di lettura/scrittura sequenziali.

Per maggiori dettagli fare riferimento al "Documentazione di Google Cloud: dischi persistenti zonali (standard e SSD)" .

Dimensione del disco

Quando si distribuisce un sistema Cloud Volumes ONTAP , è necessario scegliere una dimensione iniziale del disco. Dopodiché puoi lasciare che la NetApp Console gestisca la capacità di un sistema per te, ma se vuoi creare aggregati autonomamente, tieni presente quanto segue:

- Tutti i dischi di un aggregato devono avere le stesse dimensioni.
- Determina lo spazio di cui hai bisogno, tenendo conto delle prestazioni.
- Le prestazioni dei dischi persistenti si adattano automaticamente alle dimensioni del disco e al numero di vCPU disponibili nel sistema.

  Per maggiori dettagli fare riferimento a quanto segue:

  - "Documentazione di Google Cloud: dischi persistenti zonali (standard e SSD)"
  - "Documentazione di Google Cloud: ottimizzazione delle prestazioni del disco persistente e dell'SSD locale"

Visualizza i dischi di sistema predefiniti

Oltre allo storage per i dati utente, la Console acquista anche storage cloud per i dati di sistema Cloud Volumes ONTAP (dati di avvio, dati root, dati core e NVRAM). Ai fini della pianificazione, potrebbe essere utile rivedere questi dettagli prima di distribuire Cloud Volumes ONTAP.

- "Visualizza i dischi predefiniti per i dati di sistema Cloud Volumes ONTAP in Google Cloud" .
- "Documentazione di Google Cloud: panoramica delle quote Cloud"

  Google Cloud Compute Engine impone delle quote sull'utilizzo delle risorse, quindi assicurati di non aver raggiunto il limite prima di distribuire Cloud Volumes ONTAP.

L'agente Console richiede anche un disco di sistema. "Visualizza i dettagli sulla configurazione predefinita dell'agente della console" .

Raccogliere informazioni di rete

Quando distribuisci Cloud Volumes ONTAP in Google Cloud, devi specificare i dettagli della tua rete virtuale. Puoi utilizzare un foglio di lavoro per raccogliere le informazioni dal tuo amministratore.

Informazioni di rete per un sistema a nodo singolo

Informazioni su Google Cloud	Il tuo valore
Regione	
Zona	
Rete VPC	
Sottorete	
Criterio firewall (se ne utilizzi uno tuo)	

Informazioni di rete per una coppia HA in più zone

Informazioni su Google Cloud	Il tuo valore
Regione	
Zona per il nodo 1	
Zona per il nodo 2	
Zona per il mediatore	
VPC-0 e sottorete	
VPC-1 e sottorete	
VPC-2 e sottorete	
VPC-3 e sottorete	
Criterio firewall (se ne utilizzi uno tuo)	

Informazioni di rete per una coppia HA in una singola zona

Informazioni su Google Cloud	Il tuo valore
Regione	
Zona	
VPC-0 e sottorete	
VPC-1 e sottorete	
VPC-2 e sottorete	
VPC-3 e sottorete	
Criterio firewall (se ne utilizzi uno tuo)	

Scegli una velocità di scrittura

La Console consente di scegliere un'impostazione della velocità di scrittura per Cloud Volumes ONTAP, ad eccezione delle coppie ad alta disponibilità (HA) in Google Cloud. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normale e alta, nonché i rischi e i consigli relativi all'utilizzo di una velocità di scrittura elevata. "Scopri di più sulla velocità di scrittura" .

Scegli un profilo di utilizzo del volume

ONTAP include diverse funzionalità di efficienza di archiviazione che possono ridurre la quantità totale di spazio di archiviazione necessario. Quando si crea un volume nella Console, è possibile scegliere un profilo che abiliti queste funzionalità oppure un profilo che le disabiliti. Dovresti saperne di più su queste funzionalità per decidere quale profilo utilizzare.

Le funzionalità di efficienza dello storage NetApp offrono i seguenti vantaggi:

Provisioning sottile

Offre agli host o agli utenti più spazio di archiviazione logica di quello effettivamente disponibile nel pool di archiviazione fisico. Invece di preallocare lo spazio di archiviazione, lo spazio di archiviazione viene allocato dinamicamente a ciascun volume man mano che i dati vengono scritti.

Deduplicazione

Migliora l'efficienza individuando blocchi di dati identici e sostituendoli con riferimenti a un singolo blocco condiviso. Questa tecnica riduce i requisiti di capacità di archiviazione eliminando i blocchi ridondanti di dati che risiedono nello stesso volume.

Compressione

Riduce la capacità fisica necessaria per archiviare i dati comprimendoli all'interno di un volume su storage primario, secondario e di archivio.

Configurare la rete Google Cloud per Cloud Volumes ONTAP

La NetApp Console gestisce la configurazione dei componenti di rete per Cloud Volumes ONTAP, come indirizzi IP, maschere di rete e percorsi. È necessario assicurarsi che l'accesso a Internet in uscita sia disponibile, che siano disponibili sufficienti indirizzi IP privati, che siano attive le connessioni giuste e altro ancora.

Se si desidera distribuire una coppia HA, è necessario"Scopri come funzionano le coppie HA in Google Cloud" .

Requisiti per Cloud Volumes ONTAP

In Google Cloud devono essere soddisfatti i seguenti requisiti.

Requisiti specifici per i sistemi a nodo singolo

Se si desidera implementare un sistema a nodo singolo, assicurarsi che il networking soddisfi i seguenti requisiti.

Una VPC

È richiesto un Virtual Private Cloud (VPC) per un sistema a nodo singolo.

Indirizzi IP privati

Per un sistema a nodo singolo in Google Cloud, la Console assegna indirizzi IP privati ai seguenti:

- Nodo
- Grappolo
- VM di archiviazione
- Dati NAS LIF
- Dati iSCSI LIF

È possibile saltare la creazione del LIF di gestione della VM di archiviazione (SVM) se si distribuisce Cloud Volumes ONTAP tramite l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

Un LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessario un LIF di gestione della VM di archiviazione (SVM).

Requisiti specifici per le coppie HA

Se si desidera distribuire una coppia HA, assicurarsi che la rete soddisfi i seguenti requisiti.

Una o più zone

È possibile garantire l'elevata disponibilità dei dati distribuendo una configurazione HA su più zone o in una singola zona. Quando si crea la coppia HA, la Console chiede di scegliere più zone o una singola zona.

- Zone multiple (consigliato)

  L'implementazione di una configurazione HA su tre zone garantisce la disponibilità continua dei dati in caso di guasto in una zona. Si noti che le prestazioni di scrittura sono leggermente inferiori rispetto all'utilizzo di una singola zona, ma sono minime.

- Zona singola

  Quando distribuita in una singola zona, una configurazione Cloud Volumes ONTAP HA utilizza una politica di posizionamento distribuito. Questa politica garantisce che una configurazione HA sia protetta da un singolo punto di errore all'interno della zona, senza dover utilizzare zone separate per ottenere l'isolamento degli errori.

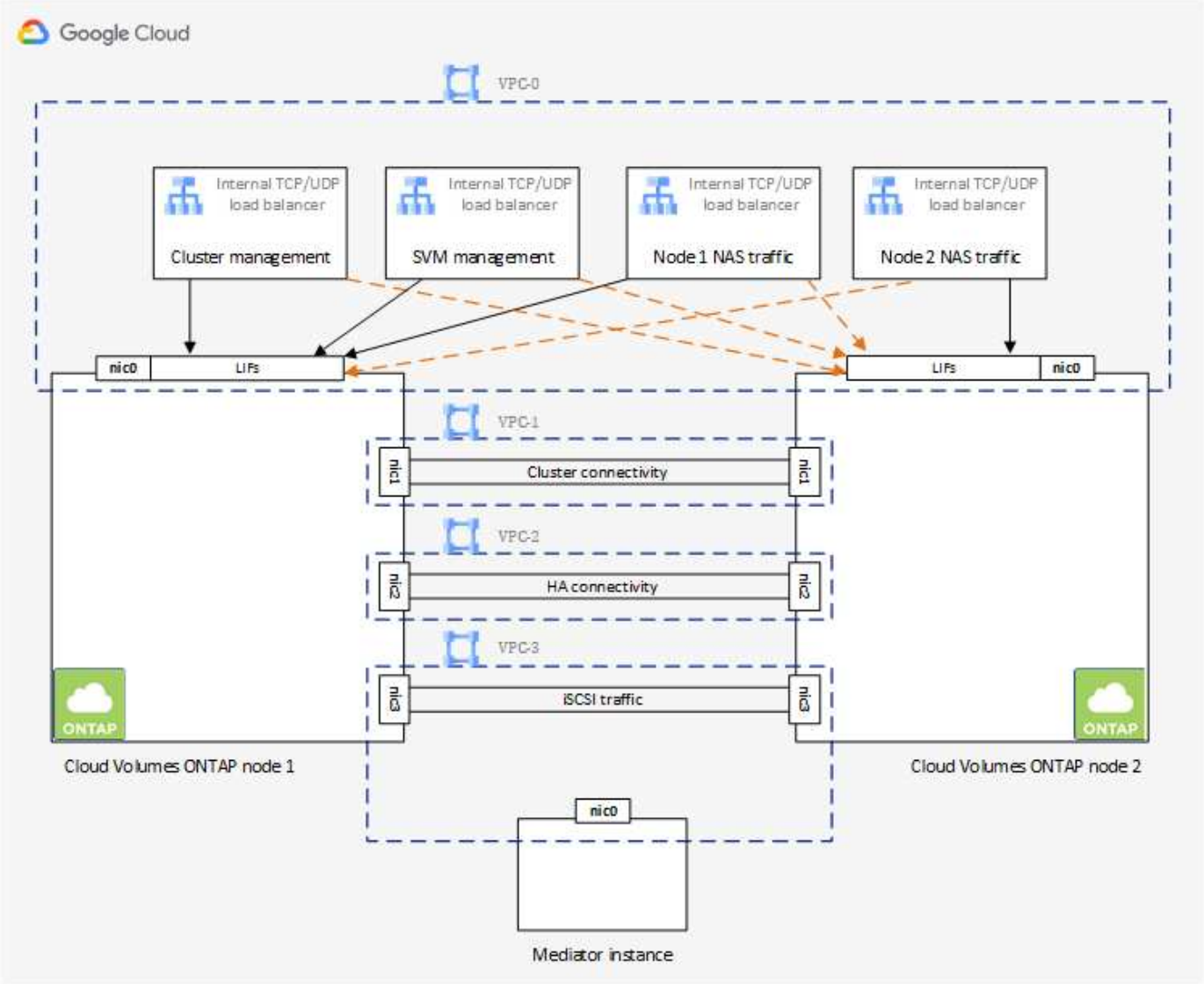
  Questo modello di distribuzione riduce i costi perché non ci sono costi per l'uscita dei dati tra le zone.

Quattro cloud privati virtuali

Per una configurazione HA sono necessari quattro Virtual Private Cloud (VPC). Sono necessarie quattro VPC perché Google Cloud richiede che ogni interfaccia di rete risieda in una rete VPC separata.

Quando si crea la coppia HA, la Console chiede di scegliere quattro VPC:

- VPC-0 per le connessioni in entrata ai dati e ai nodi
- VPC-1, VPC-2 e VPC-3 per la comunicazione interna tra i nodi e il mediatore HA



Sottoreti

Per ogni VPC è richiesta una subnet privata.

Se si posiziona l'agente della console in VPC-0, sarà necessario abilitare l'accesso privato di Google sulla subnet per accedere alle API e abilitare il tiering dei dati.

Le subnet in queste VPC devono avere intervalli CIDR distinti. Non possono avere intervalli CIDR sovrapposti.

Indirizzi IP privati

La console assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Google Cloud. Devi assicurarti che la tua rete disponga di un numero sufficiente di indirizzi privati.

Il numero di LIF allocati per Cloud Volumes ONTAP dipende dal fatto che si distribuisca un sistema a nodo singolo o una coppia HA. Un LIF è un indirizzo IP associato a una porta fisica. Un LIF di gestione SVM è necessario per strumenti di gestione come SnapCenter.

- **Singolo nodo** La NetApp Console assegna 4 indirizzi IP a un sistema a nodo singolo:
  - Gestione dei nodi LIF

- Gestione dei cluster LIF
- dati iSCSI LIF

  Un iSCSI LIF fornisce l'accesso client tramite il protocollo iSCSI e viene utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere eliminati.

- NAS LIF

  È possibile saltare la creazione del LIF di gestione della VM di archiviazione (SVM) se si distribuisce Cloud Volumes ONTAP tramite l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

- **Coppia HA** La console assegna 12-13 indirizzi IP a una coppia HA:
  - 2 LIF di gestione dei nodi (e0a)
  - 1 Gestione del cluster LIF (e0a)
  - 2 iSCSI LIF (e0a)

    Un iSCSI LIF fornisce l'accesso client tramite il protocollo iSCSI e viene utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere eliminati.

  - 1 o 2 NAS LIF (e0a)
  - 2 Cluster LIF (e0b)
  - 2 indirizzi IP di interconnessione HA (e0c)
  - 2 indirizzi IP iSCSI RSM (e0d)

    È possibile saltare la creazione del LIF di gestione della VM di archiviazione (SVM) se si distribuisce Cloud Volumes ONTAP tramite l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

Bilanciatori di carico interni

La console crea quattro bilanciatori del carico interni di Google Cloud (TCP/UDP) che gestiscono il traffico in entrata verso la coppia Cloud Volumes ONTAP HA. Non è richiesta alcuna configurazione da parte tua. Abbiamo inserito questa informazione come requisito semplicemente per informarti sul traffico di rete e per mitigare eventuali problemi di sicurezza.

Un bilanciatore del carico è per la gestione del cluster, uno è per la gestione della VM di archiviazione (SVM), uno è per il traffico NAS verso il nodo 1 e l'ultimo è per il traffico NAS verso il nodo 2.

La configurazione per ciascun bilanciatore del carico è la seguente:

- Un indirizzo IP privato condiviso
- Un controllo sanitario globale

  Per impostazione predefinita, le porte utilizzate dal controllo dello stato sono 63001, 63002 e 63003.

- Un servizio backend TCP regionale
- Un servizio di backend UDP regionale
- Una regola di inoltro TCP
- Una regola di inoltro UDP
- L'accesso globale è disabilitato

  Anche se l'accesso globale è disabilitato per impostazione predefinita, è supportata la sua abilitazione dopo la distribuzione. L'abbiamo disabilitato perché il traffico tra regioni avrà latenze significativamente più elevate. Volevamo assicurarci che non aveste esperienze negative a causa di montaggi accidentali tra regioni diverse. L'attivazione di questa opzione è specifica per le esigenze della tua azienda.

VPC condivise

Cloud Volumes ONTAP e l'agente Console sono supportati in una VPC condivisa di Google Cloud e anche in VPC autonome.

Per un sistema a nodo singolo, la VPC può essere una VPC condivisa o una VPC standalone.

Per una coppia HA sono necessarie quattro VPC. Ciascuna di queste VPC può essere condivisa o autonoma. Ad esempio, VPC-0 potrebbe essere una VPC condivisa, mentre VPC-1, VPC-2 e VPC-3 potrebbero essere VPC autonome.

Una VPC condivisa consente di configurare e gestire centralmente reti virtuali su più progetti. È possibile configurare reti VPC condivise nel *progetto host* e distribuire l'agente Console e le istanze della macchina virtuale Cloud Volumes ONTAP in un *progetto di servizio*.

"Documentazione di Google Cloud: panoramica della VPC condivisa" .

"Esaminare le autorizzazioni VPC condivise richieste trattate nella distribuzione dell'agente della console"

Mirroring dei pacchetti nelle VPC

"Mirroring dei pacchetti"deve essere disabilitato nella subnet di Google Cloud in cui distribuisci Cloud Volumes ONTAP.

Accesso a Internet in uscita

I sistemi Cloud Volumes ONTAP necessitano di accesso a Internet in uscita per accedere agli endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con requisiti di sicurezza rigorosi.

L'agente della console contatta anche diversi endpoint per le operazioni quotidiane. Per informazioni sugli endpoint, fare riferimento a "Visualizza gli endpoint contattati dall'agente della console" E "Preparare la rete per l'utilizzo della console" .

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se l'endpoint non è disponibile
\ https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione nella Console.	Modalità standard e limitata.	L'autenticazione dell'utente fallisce e i seguenti servizi rimangono non disponibili: • Servizi Cloud Volumes ONTAP • Servizi ONTAP • Protocolli e servizi proxy
\ https://api.bluexp.netapp.com/tenancy	Locazione	Utilizzato per recuperare la risorsa Cloud Volumes ONTAP dalla Console per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilizzato per inviare i dati di telemetria AutoSupport al supporto NetApp .	Modalità standard e limitata.	Le informazioni AutoSupport non vengono recapitate.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se l'endpoint non è disponibile
https://cloudbuild.googleapis.com/v1 (solo per distribuzioni in modalità privata) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (uso commerciale).	Comunicazione con i servizi Google Cloud.	Modalità standard, limitata e privata.	Cloud Volumes ONTAP non riesce a comunicare con il servizio Google Cloud per eseguire operazioni specifiche per la Console in Google Cloud.

Connessioni ai sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in Google Cloud e sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra la VPC e l'altra rete, ad esempio la rete aziendale.

"Documentazione di Google Cloud: panoramica di Cloud VPN" .

Regole del firewall

La console crea regole firewall di Google Cloud che includono le regole in entrata e in uscita di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. Potresti voler fare riferimento alle porte a scopo di test o se preferisci utilizzare le tue regole firewall.

Le regole del firewall per Cloud Volumes ONTAP richiedono regole sia in entrata che in uscita. Se si sta distribuendo una configurazione HA, queste sono le regole del firewall per Cloud Volumes ONTAP in VPC-0.

Si noti che per una configurazione HA sono necessari due set di regole del firewall:

- Un set di regole per i componenti HA in VPC-0. Queste regole consentono l'accesso ai dati su Cloud Volumes ONTAP.
- Un altro set di regole per i componenti HA in VPC-1, VPC-2 e VPC-3. Queste regole sono aperte alla comunicazione in entrata e in uscita tra i componenti HA. Saperne di più .

Cerchi informazioni sull'agente Console? "Visualizza le regole del firewall per l'agente della console"

Regole in entrata

Quando si aggiunge un sistema Cloud Volumes ONTAP , è possibile scegliere il filtro di origine per la policy firewall predefinita durante la distribuzione:

- **Solo VPC selezionata**: il filtro di origine per il traffico in entrata è l'intervallo di subnet della VPC per il sistema Cloud Volumes ONTAP e l'intervallo di subnet della VPC in cui risiede l'agente della console. Questa è l'opzione consigliata.
- **Tutte le VPC**: il filtro di origine per il traffico in entrata è l'intervallo IP 0.0.0.0/0.

Se utilizzi una tua policy firewall, assicurati di aggiungere tutte le reti che devono comunicare con Cloud Volumes ONTAP, ma assicurati anche di aggiungere entrambi gli intervalli di indirizzi per consentire al Google Load Balancer interno di funzionare correttamente. Questi indirizzi sono 130.211.0.0/22 e 35.191.0.0/16. Per maggiori informazioni, fare riferimento al "Documentazione di Google Cloud: regole del firewall del bilanciatore del carico" .

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di ONTAP System Manager tramite l'indirizzo IP del LIF di gestione del cluster
HTTPS	443	Connettività con l'agente Console e accesso HTTPS alla console Web ONTAP System Manager utilizzando l'indirizzo IP del LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione del nodo
TCP	111	Chiamata di procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo semplice di gestione della rete
TCP	445	Microsoft SMB/CIFS su TCP con framing NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Demone del server NFS
TCP	3260	Accesso iSCSI tramite i dati iSCSI LIF
TCP	4045	Demone di blocco NFS

Protocollo	Porta	Scopo
TCP	4046	Monitoraggio dello stato di rete per NFS
TCP	10000	Backup tramite NDMP
TCP	11104	Gestione delle sessioni di comunicazione intercluster per SnapMirror
TCP	11105	Trasferimento dati SnapMirror tramite LIF intercluster
TCP	63001-63050	Porte di sonda per il bilanciamento del carico per determinare quale nodo è integro (richiesto solo per coppie HA)
UDP	111	Chiamata di procedura remota per NFS
UDP	161-162	Protocollo semplice di gestione della rete
UDP	635	Montaggio NFS
UDP	2049	Demone del server NFS
UDP	4045	Demone di blocco NFS
UDP	4046	Monitoraggio dello stato di rete per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti gli TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se hai bisogno di regole rigide per il traffico in uscita, puoi utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte di Cloud Volumes ONTAP. I cluster Cloud Volumes ONTAP utilizzano le seguenti porte per regolare il traffico dei nodi.

La sorgente è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP .

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
Directory attiva	TCP	88	Gestione dei nodi LIF	Foresta di Active Directory	Autenticazione Kerberos V
	UDP	137	Gestione dei nodi LIF	Foresta di Active Directory	Servizio di denominazione NetBIOS
	UDP	138	Gestione dei nodi LIF	Foresta di Active Directory	Servizio datagramma NetBIOS
	TCP	139	Gestione dei nodi LIF	Foresta di Active Directory	Sessione del servizio NetBIOS
	TCP e UDP	389	Gestione dei nodi LIF	Foresta di Active Directory	LDAP
	TCP	445	Gestione dei nodi LIF	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	TCP	464	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	UDP	464	Gestione dei nodi LIF	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)
	TCP	88	Dati LIF (NFS, CIFS, iSCSI)	Foresta di Active Directory	Autenticazione Kerberos V
	UDP	137	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio di denominazione NetBIOS
	UDP	138	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio datagramma NetBIOS
	TCP	139	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Sessione del servizio NetBIOS
	TCP e UDP	389	Dati LIF (NFS, CIFS)	Foresta di Active Directory	LDAP
	TCP	445	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	TCP	464	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	UDP	464	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
AutoSupport	HTTPS	443	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	Gestione dei nodi LIF	Agente console	Invio di messaggi AutoSupport tramite un server proxy sull'agente Console, se non è disponibile una connessione Internet in uscita
Backup di configurazione	HTTP	80	Gestione dei nodi LIF	http://<indirizzo-IP-agente-console>/occm/offboxconfig	Inviare i backup della configurazione all'agente della console."Documentazione ONTAP"
DHCP	UDP	68	Gestione dei nodi LIF	DHCP	Client DHCP per la prima configurazione
DHCP	UDP	67	Gestione dei nodi LIF	DHCP	server DHCP
DNS	UDP	53	Gestione dei nodi LIF e dati LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Gestione dei nodi LIF	Server di destinazione	Copia NDMP
SMTP	TCP	25	Gestione dei nodi LIF	Server di posta	Avvisi SMTP, possono essere utilizzati per AutoSupport
SNMP	TCP	161	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	UDP	161	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	TCP	162	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	UDP	162	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
SnapMirror	TCP	11104	Intercluster LIF	LIF intercluster ONTAP	Gestione delle sessioni di comunicazione intercluster per SnapMirror
	TCP	11105	Intercluster LIF	LIF intercluster ONTAP	Trasferimento dati SnapMirror
Registro di sistema	UDP	514	Gestione dei nodi LIF	Server Syslog	Messaggi di inoltro Syslog

Regole per VPC-1, VPC-2 e VPC-3

In Google Cloud, una configurazione HA viene distribuita su quattro VPC. Le regole del firewall necessarie per la configurazione HA in VPC-0 sonoelencati sopra per Cloud Volumes ONTAP .

Nel frattempo, le regole firewall predefinite create per le istanze in VPC-1, VPC-2 e VPC-3 abilitano la comunicazione in ingresso su *tutti* i protocolli e le porte. Queste regole consentono la comunicazione tra nodi HA.

La comunicazione dai nodi HA al mediatore HA avviene tramite la porta 3260 (iSCSI).

> Per consentire un'elevata velocità di scrittura per le nuove distribuzioni di coppie Google Cloud HA, è richiesta un'unità di trasmissione massima (MTU) di almeno 8.896 byte per VPC-1, VPC-2 e VPC-3. Se si sceglie di aggiornare VPC-1, VPC-2 e VPC-3 esistenti a un MTU di 8.896 byte, è necessario arrestare tutti i sistemi HA esistenti che utilizzano queste VPC durante il processo di configurazione.

Configurazione di Infrastructure Manager per distribuzioni in modalità privata

Se si desidera distribuire Cloud Volumes ONTAP 9.16.1 o versioni successive in modalità privata, è necessario apportare alcune modifiche alla configurazione in modo che Cloud Volumes ONTAP possa utilizzare Google Cloud Infrastructure Manager come servizio di distribuzione invece di Deployment Manager, che Google alla fine disattiverà.

Prima di iniziare

- Assicurati che il tuo sistema Cloud Volumes ONTAP sia 9.16.1 o successivo. Se non lo è, aggiorna il sistema. Consulta "Aggiorna Cloud Volumes ONTAP" per le istruzioni.
- Assicurati che le API di Google Cloud siano abilitate. Fare riferimento a "Abilita le API di Google Cloud".
- Assicurati che l'API Cloud Build sia abilitata. Fai riferimento a "Abilita qui l'API Cloud Build".
- Verificare che l'account di servizio dell'agente Console disponga di tutte le autorizzazioni standard. Assicurarsi inoltre che l'account di servizio disponga delle autorizzazioni `cloudbuild.workerpools.get` e `cloudbuild.workerpools.list`. Fare riferimento a "Autorizzazioni di Google Cloud per l'agente della console".

Passi

1. Crea un pool di worker privato con questa configurazione nella stessa regione delle distribuzioni Cloud Volumes ONTAP. Per informazioni sulla creazione di un pool di worker privato, fare riferimento a "Documentazione Google Cloud: creare e gestire pool privati" e "Prezzi di Google Cloud Build".

   Il pool di worker deve avere la seguente configurazione:

   - Tipo di macchina: e2-medium
   - Dimensione del disco: 100 GB
   - Assegna IP esterno: False
   - Rete: predefinita o una privata.
   - La subnet configurata per accedere "Google APIs". Esegui questi passaggi per assicurarti che la subnet possa accedere alle Google API:
     i. Assicurarsi che "Private Google Access" sia attivato per la subnet.
     ii. Vai a **VPC Network level > Scheda Private Service Access > Allocated IP ranges for services**.

iii. Seleziona **Allocate IP range** e assegna l'intervallo IP interno per la connessione privata al Google Compute Service.

iv. In **Connessione privata ai servizi**, seleziona **Crea connessione**.

v. Seleziona **Connected service producer = Google Cloud Platform**.

vi. Assegna l'allocazione per l'intervallo IP di connessione privata che hai creato nel passaggio precedente.

2. Distribuisci questo pool di worker e mantienilo in esecuzione per la gestione di Cloud Volumes ONTAP. Google Cloud utilizza questo pool di worker per eseguire tutte le operazioni Terraform in un ambiente isolato.
3. Quando si distribuisce Cloud Volumes ONTAP in modalità privata, selezionare il nome di questo worker pool nel campo **GCP Worker Pool**. Fare riferimento a "Avvia Cloud Volumes ONTAP in Google Cloud" per le istruzioni.

Requisiti per l'agente della console

Se non hai ancora creato un agente Console, dovresti rivedere i requisiti di rete.

- "Visualizza i requisiti di rete per l'agente della console"
- "Regole del firewall in Google Cloud"

Configurazioni di rete per supportare il proxy dell'agente della console

È possibile utilizzare i server proxy configurati per l'agente Console per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. La console supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy dell'agente della console. L'amministratore dell'agente della console potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato sul sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.
- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP tramite il proxy dell'agente della console. Quando si configura un proxy trasparente, l'amministratore dell'agente della console deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurati di ottenere e caricare lo stesso certificato CA radice sul tuo sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy per l'agente Console, fare riferimento a "Configurare un agente Console per utilizzare un server proxy" .

Configurare i tag di rete per Cloud Volumes ONTAP in Google Cloud

Durante la configurazione del proxy trasparente dell'agente Console, l'amministratore aggiunge un tag di rete per Google Cloud. È necessario ottenere e aggiungere manualmente lo stesso tag di rete per la configurazione Cloud Volumes ONTAP . Questo tag è necessario per il corretto funzionamento del server proxy.

1. Nella Google Cloud Console, individua il tuo sistema Cloud Volumes ONTAP.
2. Vai a **Dettagli > Networking > Tag di rete**.
3. Aggiungere il tag utilizzato per l'agente Console e salvare la configurazione.

Argomenti correlati

- "Verifica la configurazione AutoSupport per Cloud Volumes ONTAP"
- "Scopri di più sulle porte interne ONTAP" .

Configurare i controlli del servizio VPC per distribuire Cloud Volumes ONTAP in Google Cloud

Quando si sceglie di bloccare l'ambiente Google Cloud con VPC Service Controls, è necessario comprendere come NetApp Console e Cloud Volumes ONTAP interagiscono con le API di Google Cloud, nonché come configurare il perimetro del servizio per distribuire Console e Cloud Volumes ONTAP.

I controlli del servizio VPC consentono di controllare l'accesso ai servizi gestiti da Google al di fuori di un perimetro attendibile, di bloccare l'accesso ai dati da posizioni non attendibili e di mitigare i rischi di trasferimento dati non autorizzato. "Scopri di più sui controlli del servizio VPC di Google Cloud" .

Come i servizi NetApp comunicano con i controlli del servizio VPC

La Console comunica direttamente con le API di Google Cloud. Questa operazione può essere attivata da un indirizzo IP esterno a Google Cloud (ad esempio, da api.services.cloud.netapp.com) oppure all'interno di Google Cloud da un indirizzo interno assegnato all'agente della console.

A seconda dello stile di distribuzione dell'agente della console, potrebbe essere necessario effettuare alcune eccezioni per il perimetro del servizio.

Immagini

Sia Cloud Volumes ONTAP che la Console utilizzano immagini provenienti da un progetto all'interno di Google Cloud gestito da NetApp. Ciò può influire sulla distribuzione dell'agente della Console e di Cloud Volumes ONTAP, se l'organizzazione dispone di una policy che blocca l'utilizzo di immagini non ospitate all'interno dell'organizzazione.

È possibile distribuire manualmente un agente Console utilizzando il metodo di installazione manuale, ma Cloud Volumes ONTAP dovrà anche estrarre le immagini dal progetto NetApp . Per poter distribuire un agente Console e Cloud Volumes ONTAP, è necessario fornire un elenco consentito.

Distribuzione di un agente console

L'utente che distribuisce un agente Console deve essere in grado di fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e nel numero di progetto *14190056516*.

Distribuzione di Cloud Volumes ONTAP

- L'account del servizio Console deve fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516* del progetto del servizio.
- L'account di servizio per l'agente di servizio predefinito delle API di Google deve fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516* dal progetto di servizio.

Di seguito sono definiti alcuni esempi delle regole necessarie per estrarre queste immagini con VPC Service Controls.

Criteri perimetrali dei controlli del servizio VPC

Le policy consentono eccezioni ai set di regole dei VPC Service Controls. Per ulteriori informazioni sulle policy, visitare il "Documentazione sui criteri di controllo del servizio VPC di Google Cloud".

Per impostare i criteri richiesti dalla Console, accedi al perimetro dei controlli del servizio VPC all'interno della tua organizzazione e aggiungi i seguenti criteri. I campi devono corrispondere alle opzioni fornite nella pagina dei criteri di controllo del servizio VPC. Si noti inoltre che **tutte** le regole sono obbligatorie e che nel set di regole devono essere utilizzati i parametri **OR**.

Regole di ingresso

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

O

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

O

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Regole di uscita

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Il numero di progetto sopra indicato è il progetto *netapp-cloudmanager* utilizzato da NetApp per archiviare le immagini per l'agente Console e per Cloud Volumes ONTAP.

Crea un account di servizio Google Cloud per Cloud Volumes ONTAP

Cloud Volumes ONTAP richiede un account di servizio Google Cloud per due scopi. Il primo è quando abiliti"livelli di dati" per suddividere i dati inutilizzati in un archivio di oggetti a basso costo su Google Cloud. Il secondo è quando si abilita il "NetApp Backup and Recovery" per eseguire il backup di volumi su storage di oggetti a basso costo.

Cloud Volumes ONTAP utilizza l'account di servizio per accedere e gestire un bucket per i dati a livelli e un altro bucket per i backup.

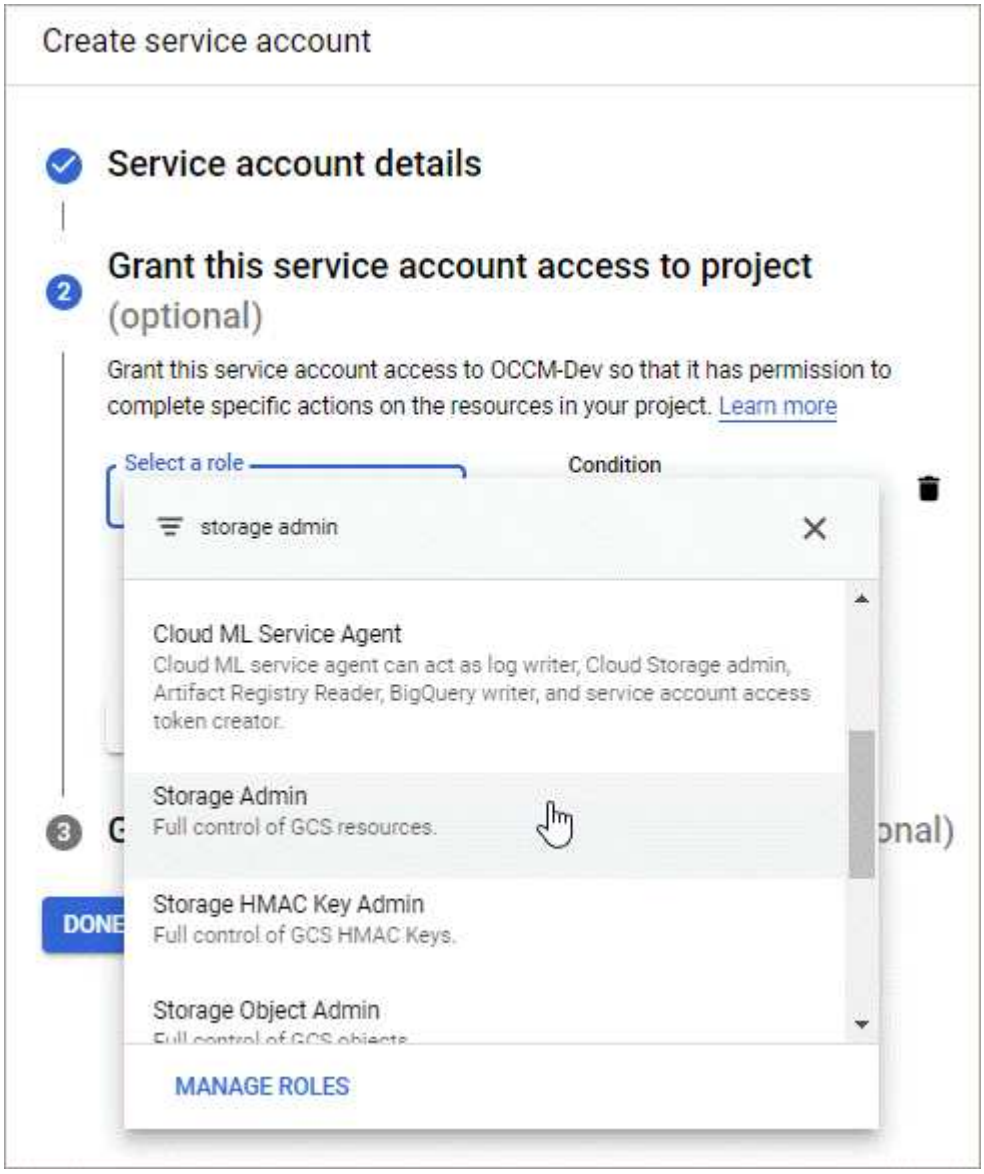
È possibile configurare un account di servizio e utilizzarlo per entrambi gli scopi. L'account di servizio deve avere il ruolo **Amministratore archiviazione**.

Passi

1. Nella Google Cloud Console, "vai alla pagina Account di servizio".
2. Seleziona il tuo progetto.
3. Fare clic su **Crea account di servizio** e fornire le informazioni richieste.

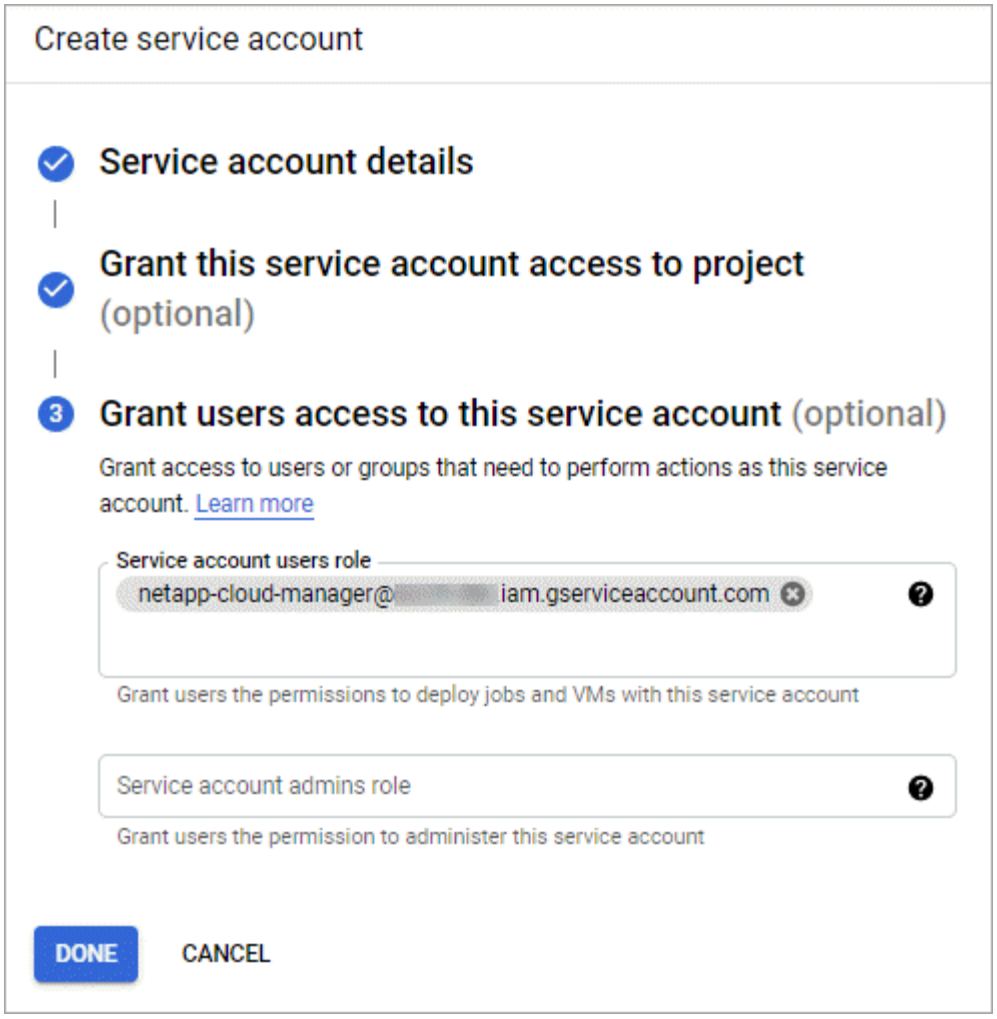
a. **Dettagli dell'account di servizio**: inserisci un nome e una descrizione.

b. **Concedi a questo account di servizio l'accesso al progetto**: seleziona il ruolo **Amministratore archiviazione**.



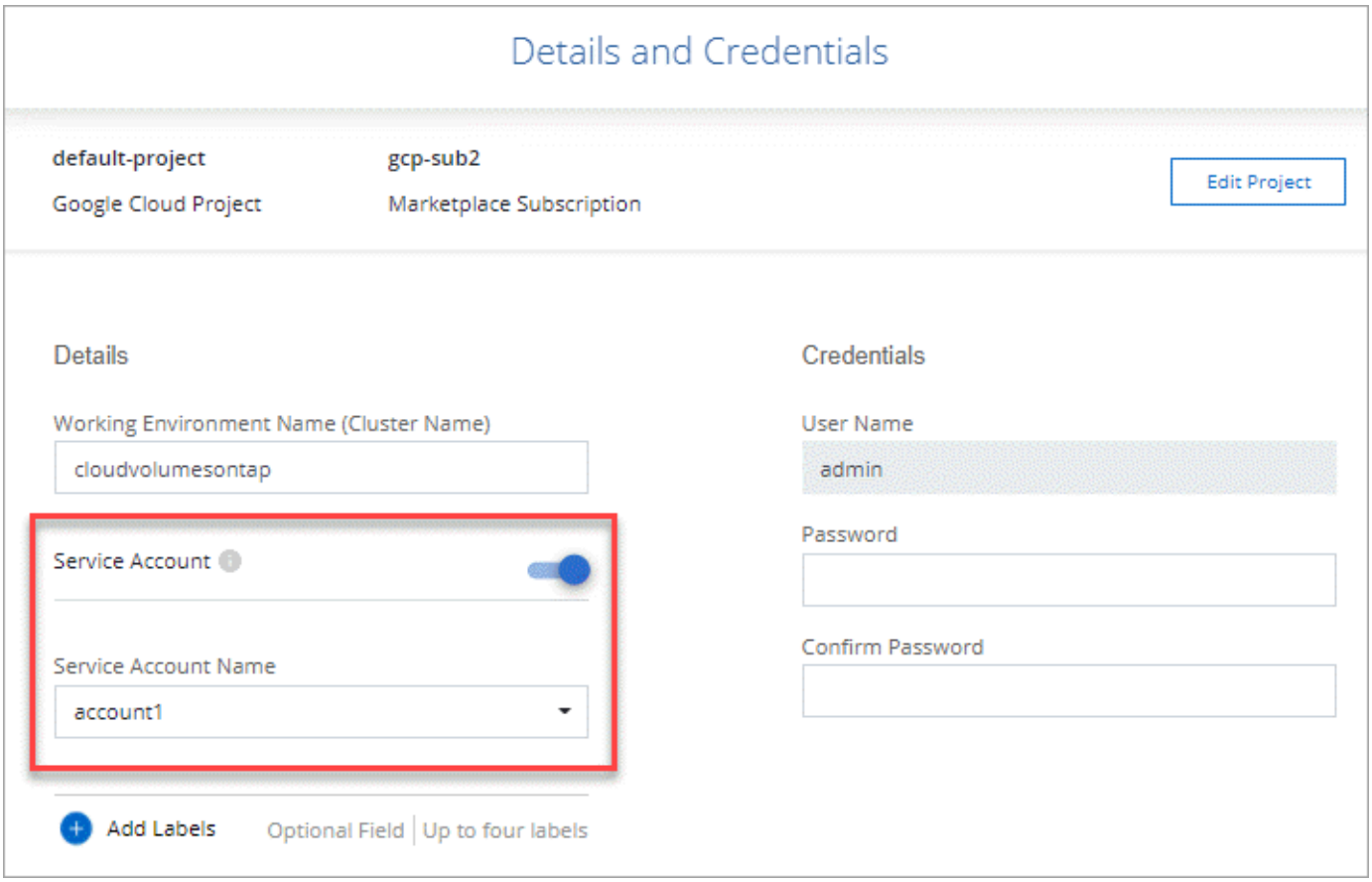
c. **Concedi agli utenti l'accesso a questo account di servizio**: aggiungi l'account di servizio dell'agente della console come *Utente account di servizio* a questo nuovo account di servizio.

   Questo passaggio è necessario solo per la suddivisione in livelli dei dati. Non è necessario per il backup e il ripristino.



Cosa succederà ora?

Sarà necessario selezionare l'account di servizio in un secondo momento, quando si crea un sistema Cloud Volumes ONTAP .



Utilizzo di chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP

Sebbene Google Cloud Storage crittografi sempre i dati prima che vengano scritti sul disco, è possibile utilizzare le API per creare un sistema Cloud Volumes ONTAP che utilizzi *chiavi di crittografia gestite dal cliente*. Si tratta di chiavi che puoi generare e gestire in GCP utilizzando Cloud Key Management Service.

Passi

1. Assicurarsi che l'account del servizio agente della console disponga delle autorizzazioni corrette a livello di progetto, nel progetto in cui è archiviata la chiave.

   I permessi sono forniti nel "le autorizzazioni dell'account di servizio per impostazione predefinita" , ma potrebbe non essere applicato se si utilizza un progetto alternativo per il Cloud Key Management Service.

   I permessi sono i seguenti:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Assicurarsi che l'account di servizio per il "Agente di servizio Google Compute Engine" dispone delle autorizzazioni Cloud KMS Encrypter/Decrypter sulla chiave.

Il nome dell'account di servizio utilizza il seguente formato: "service-[service_project_number]@compute-system.iam.gserviceaccount.com".

"Documentazione di Google Cloud: Utilizzo di IAM con Cloud KMS - Concessione di ruoli su una risorsa"

3. Ottieni l'"id" della chiave invocando il comando get per `/gcp/vsa/metadata/gcp-encryption-keys` Chiamata API o selezionando "Copia nome risorsa" sulla chiave nella console GCP.
4. Se si utilizzano chiavi di crittografia gestite dal cliente e si suddividono i dati in livelli per l'archiviazione di oggetti, la NetApp Console tenta di utilizzare le stesse chiavi utilizzate per crittografare i dischi persistenti. Ma prima devi abilitare i bucket di Google Cloud Storage per utilizzare le chiavi:

   a. Trova l'agente del servizio Google Cloud Storage seguendo le istruzioni "Documentazione di Google Cloud: ottenere l'agente del servizio Cloud Storage" .

   b. Passare alla chiave di crittografia e assegnare all'agente del servizio Google Cloud Storage le autorizzazioni Cloud KMS Encrypter/Decrypter.

   Per maggiori informazioni, fare riferimento a "Documentazione di Google Cloud: utilizzo delle chiavi di crittografia gestite dal cliente"

5. Utilizza il parametro ""gcpEncryption"" con la richiesta API durante la creazione di un sistema.

   Esempio

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Fare riferimento al "Documentazione sull'automazione NetApp Console" per maggiori dettagli sull'utilizzo del parametro "GcpEncryption".

Impostare le licenze per Cloud Volumes ONTAP in Google Cloud

Dopo aver deciso quale opzione di licenza utilizzare con Cloud Volumes ONTAP, sono necessari alcuni passaggi prima di poter scegliere tale opzione di licenza durante la creazione di un nuovo sistema.

Freemium

Seleziona l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con una capacità fornita fino a 500 GiB. "Scopri di più sull'offerta Freemium" .

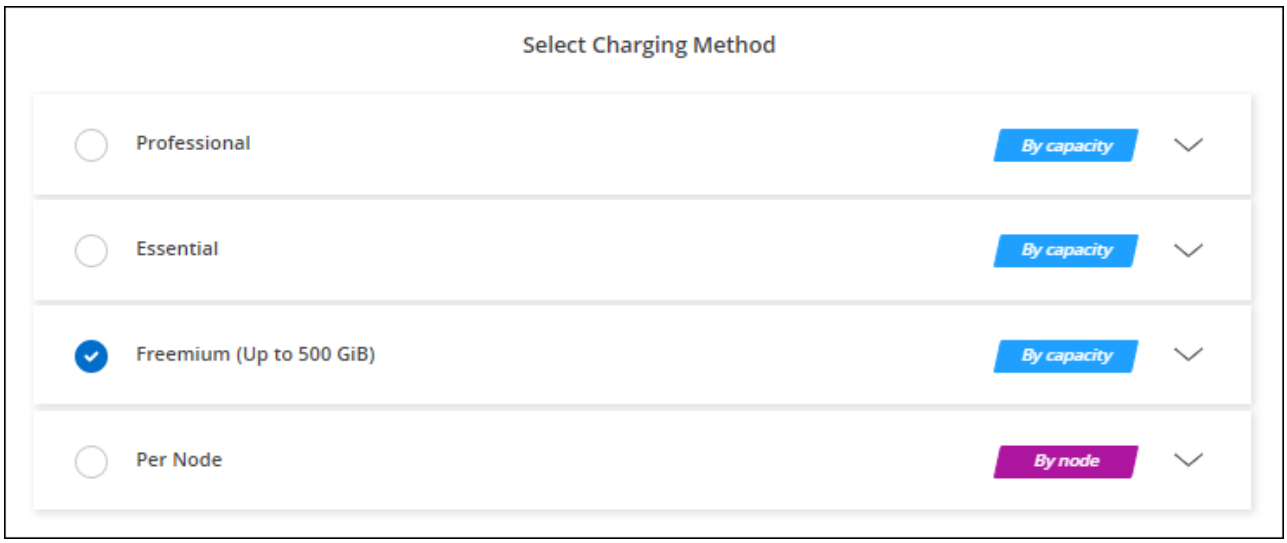
Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi nella NetApp Console.
   a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti all'offerta a pagamento in Google Cloud Marketplace.

      Non ti verrà addebitato alcun costo tramite l'abbonamento al marketplace a meno che tu non superi i 500 GiB di capacità fornita, momento in cui il sistema verrà automaticamente convertito in"Pacchetto

essenziale" .

b. Dopo essere tornato alla Console, seleziona **Freemium** quando arrivi alla pagina dei metodi di addebito.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud" .

Licenza basata sulla capacità

Le licenze basate sulla capacità consentono di pagare Cloud Volumes ONTAP per TiB di capacità. Le licenze basate sulla capacità sono disponibili sotto forma di *pacchetto*: il pacchetto Essentials o Professional.

I pacchetti Essentials e Professional sono disponibili con i seguenti modelli di consumo o opzioni di acquisto:

- Una licenza (Bring Your Own License (BYOL)) acquistata da NetApp
- Un abbonamento orario a consumo (PAYGO) da Google Cloud Marketplace
- Un contratto annuale

"Scopri di più sulle licenze basate sulla capacità" .

Le sezioni seguenti descrivono come iniziare a utilizzare ciascuno di questi modelli di consumo.

BYOL

Paga in anticipo acquistando una licenza (BYOL) da NetApp per distribuire i sistemi Cloud Volumes ONTAP in qualsiasi provider cloud.

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Passi

1. "Contatta NetApp Sales per ottenere una licenza"
2. "Aggiungi il tuo account del sito di supporto NetApp alla NetApp Console"

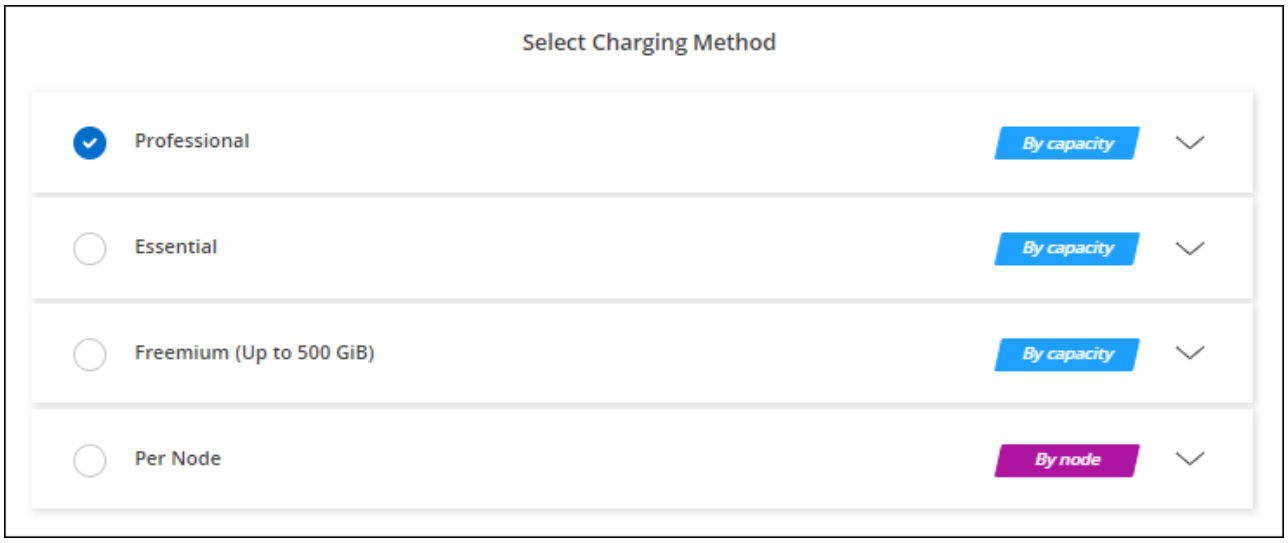
   La Console interroga automaticamente il servizio licenze di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. Se non ci sono errori, la Console aggiunge le licenze.

La licenza deve essere disponibile nella Console prima di poterla utilizzare con Cloud Volumes ONTAP. Se necessario, puoi"aggiungere manualmente la licenza alla Console" .

3. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti all'offerta a pagamento in Google Cloud Marketplace.

      La licenza acquistata da NetApp viene sempre addebitata per prima, ma ti verrà addebitata la tariffa oraria del marketplace se superi la capacità della licenza o se scade il termine della licenza.

   b. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud" .

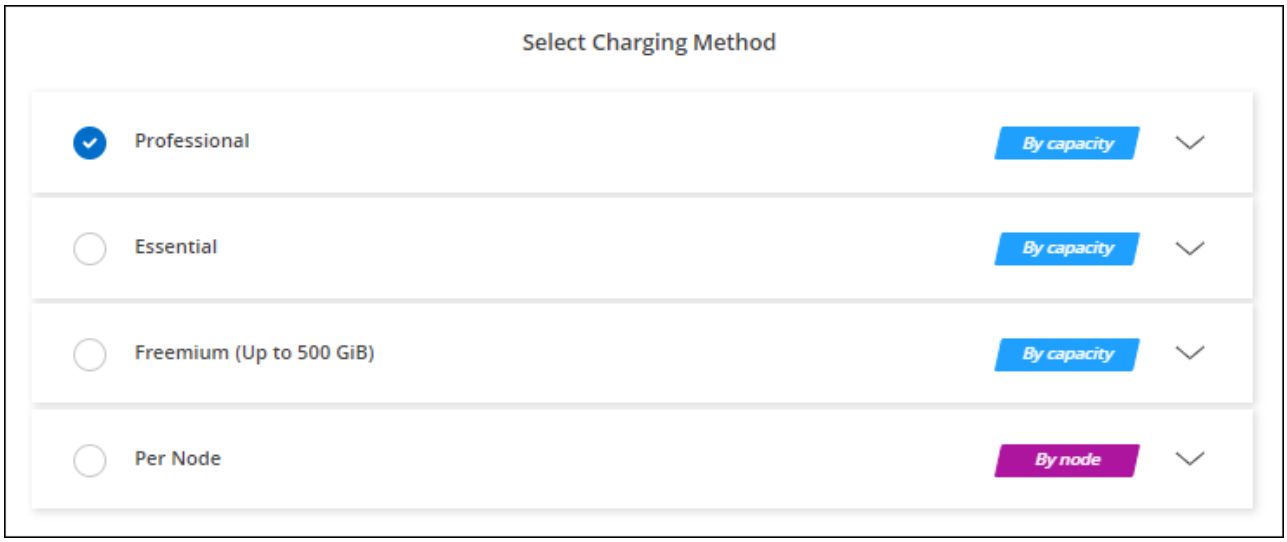
Abbonamento PAYGO

Paga a ore sottoscrivendo l'offerta dal marketplace del tuo provider cloud.

Quando si crea un sistema Cloud Volumes ONTAP , la Console richiede di sottoscrivere il contratto disponibile in Google Cloud Marketplace. Tale abbonamento viene poi associato al sistema di addebito. È possibile utilizzare lo stesso abbonamento per sistemi aggiuntivi.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti all'offerta a pagamento in Google Cloud Marketplace.
   b. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud" .

Puoi gestire gli abbonamenti a Google Cloud Marketplace associati ai tuoi account dalla pagina Impostazioni > Credenziali. "Scopri come gestire le tue credenziali e i tuoi abbonamenti Google Cloud"

Contratto annuale

Paga annualmente Cloud Volumes ONTAP acquistando un contratto annuale.

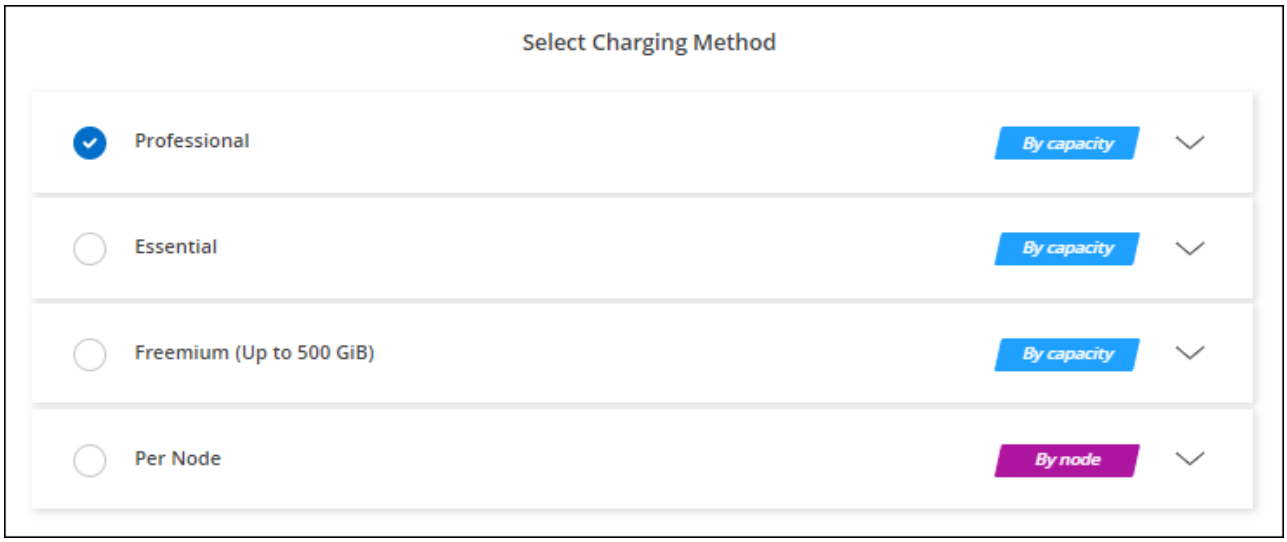
Passi

1. Contatta il tuo rappresentante commerciale NetApp per acquistare un contratto annuale.

   Il contratto è disponibile come offerta *privata* nel Google Cloud Marketplace.

   Dopo che NetApp avrà condiviso con te l'offerta privata, potrai selezionare il piano annuale quando ti iscrivi da Google Cloud Marketplace durante la creazione del sistema.

2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
   a. Nella pagina **Dettagli e credenziali**, fai clic su **Modifica credenziali > Aggiungi abbonamento** e segui le istruzioni per abbonarti al piano annuale in Google Cloud Marketplace.
   b. In Google Cloud, seleziona il piano annuale condiviso con il tuo account, quindi fai clic su **Iscriviti**.
   c. Dopo essere tornati alla Console, selezionate un pacchetto basato sulla capacità quando raggiungete la pagina dei metodi di ricarica.



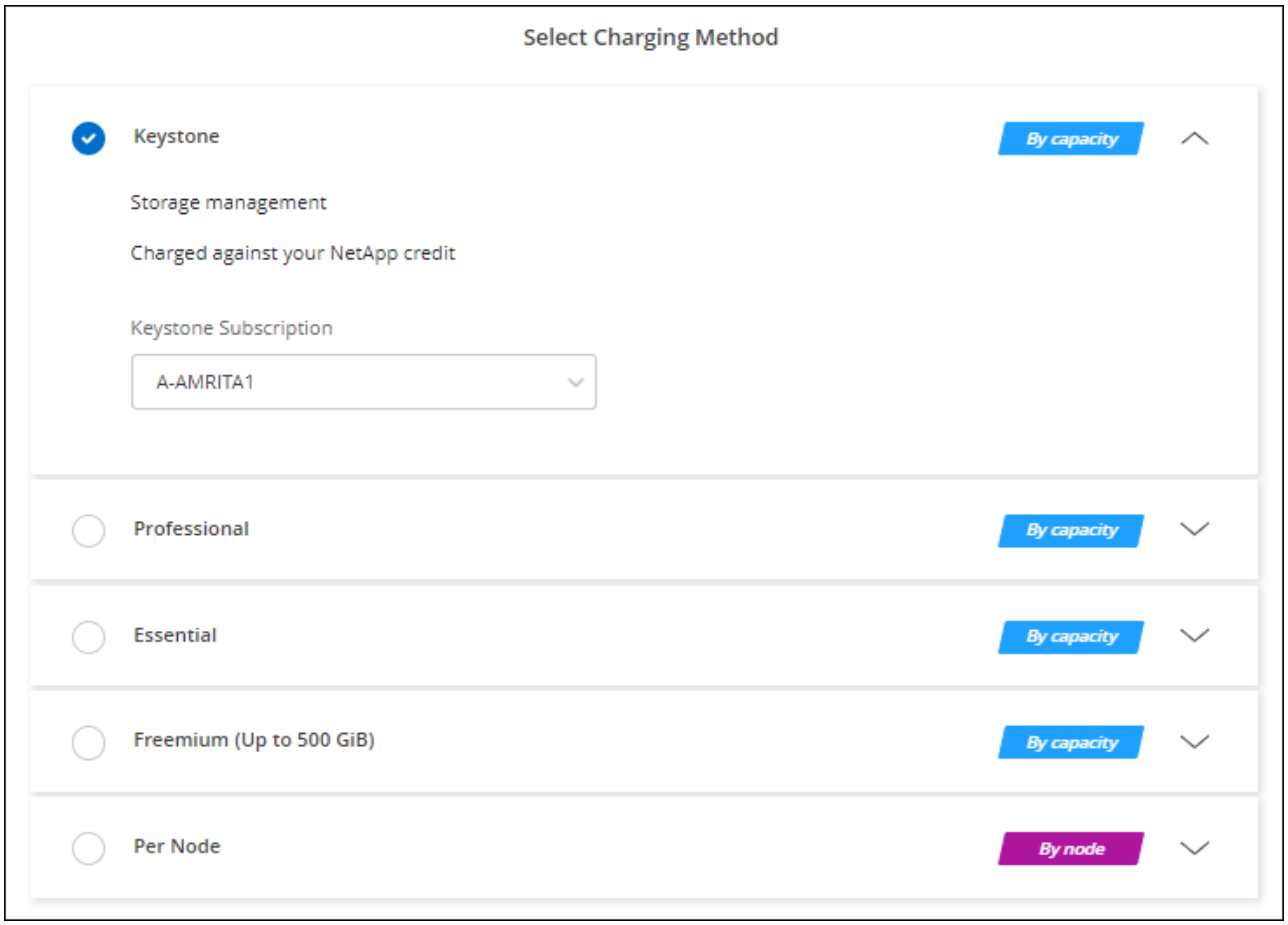
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud" .

Abbonamento Keystone

Un abbonamento Keystone è un servizio basato su un abbonamento con pagamento in base alla crescita. "Scopri di più sugli abbonamenti NetApp Keystone" .

Passi

1. Se non hai ancora un abbonamento, "contattare NetApp"
2. Contatta NetApp per autorizzare il tuo account utente Console con uno o più abbonamenti Keystone .
3. Dopo che NetApp autorizza il tuo account,"collega i tuoi abbonamenti per utilizzarli con Cloud Volumes ONTAP" .
4. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire i passaggi.
    a. Quando ti viene richiesto di scegliere un metodo di addebito, seleziona il metodo di addebito Keystone Subscription.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud" .

Licenza basata su nodi

Una licenza basata su nodi è la licenza di precedente generazione per Cloud Volumes ONTAP. Una licenza basata su nodi può essere acquistata da NetApp (BYOL) ed è disponibile per i rinnovi di licenza solo in casi specifici. Per informazioni, fare riferimento a:

- "Fine della disponibilità delle licenze basate su nodi"
- "Fine della disponibilità delle licenze basate sui nodi"
- "Convertire una licenza basata su nodi in una licenza basata sulla capacità"

Avvia Cloud Volumes ONTAP in Google Cloud

È possibile avviare Cloud Volumes ONTAP in una configurazione a nodo singolo o come coppia HA in Google Cloud.

Prima di iniziare

Prima di iniziare, ti occorre quanto segue.

- Un agente NetApp Console attivo e funzionante.
  - Dovresti avere un "Agente console associato al tuo sistema" .
  - "Dovresti essere pronto a lasciare l'agente della console sempre in esecuzione" .

- L’account di servizio associato all’agente della console "dovrebbe avere i permessi richiesti"

- Una comprensione della configurazione che si desidera utilizzare.

  Dovresti esserti preparato scegliendo una configurazione e ottenendo le informazioni di rete di Google Cloud dal tuo amministratore. Per i dettagli, fare riferimento a"Pianificazione della configurazione Cloud Volumes ONTAP" .

- Una comprensione di ciò che è necessario per impostare la licenza per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze" .

- Le API di Google Cloud dovrebbero essere "abilitato nel tuo progetto" :
  - API di Cloud Deployment Manager V2
  - API di registrazione cloud
  - API di Cloud Resource Manager
  - API di Compute Engine
  - API di gestione dell’identità e dell’accesso (IAM)

Avvia un sistema a nodo singolo in Google Cloud

Crea un sistema nella NetApp Console per avviare Cloud Volumes ONTAP in Google Cloud.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Aggiungi sistema** e seguire le istruzioni.
3. **Scegli una posizione**: seleziona **Google Cloud** e * Cloud Volumes ONTAP*.
4. Se richiesto, "creare un agente Console" .
5. **Dettagli e credenziali**: seleziona un progetto, specifica un nome per il cluster, seleziona facoltativamente un account di servizio, aggiungi facoltativamente delle etichette e quindi specifica le credenziali.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia l’istanza Google Cloud VM. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.
Nome dell’account di servizio	Se hai intenzione di utilizzare"livelli di dati" O "NetApp Backup and Recovery" con Cloud Volumes ONTAP, è necessario abilitare **Account di servizio** e selezionare un account di servizio che abbia il ruolo di amministratore di archiviazione predefinito. "Scopri come creare un account di servizio" .
Aggiungi etichette	Le etichette sono metadati per le tue risorse Google Cloud. La console aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse Google Cloud associate al sistema. È possibile aggiungere fino a quattro etichette dall’interfaccia utente durante la creazione di un sistema, per poi aggiungerne altre dopo la creazione. Tieni presente che l’API non ti limita a quattro etichette quando crei un sistema. Per informazioni sulle etichette, fare riferimento a "Documentazione di Google Cloud: Etichettatura delle risorse" .

Campo	Descrizione
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.
Modifica progetto	Seleziona il progetto in cui desideri che risieda Cloud Volumes ONTAP . Il progetto predefinito è il progetto in cui si trova la Console. Se non vedi altri progetti nell'elenco a discesa, significa che non hai ancora associato l'account di servizio ad altri progetti. Vai alla Google Cloud Console, apri il servizio IAM e seleziona il progetto. Aggiungi l'account di servizio con il ruolo che usi per la Console a quel progetto. Dovrai ripetere questo passaggio per ogni progetto. Questo è l'account di servizio che hai configurato per la Console,"come descritto in questa pagina" . Fare clic su **Aggiungi abbonamento** per associare le credenziali selezionate a un abbonamento. Per creare un sistema Cloud Volumes ONTAP con pagamento in base al consumo, è necessario selezionare un progetto Google Cloud associato a un abbonamento a Cloud Volumes ONTAP dal marketplace di Google Cloud. Fare riferimento a "Associazione di un abbonamento al marketplace alle credenziali di Google Cloud" .

6. **Servizi**: seleziona i servizi che desideri utilizzare su questo sistema. Per selezionare Backup e ripristino o per utilizzare NetApp Cloud Tiering, è necessario aver specificato l'account di servizio nel passaggio 3.

   Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

7. **Posizione e connettività**: seleziona la regione e la zona di Google Cloud per il tuo sistema, scegli una policy firewall e conferma la connettività di rete allo storage di Google Cloud per il data tiering.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Verifica della connettività	Per suddividere i dati inattivi in un bucket di Google Cloud Storage, la subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per le istruzioni, fare riferimento a "Documentazione di Google Cloud: configurazione dell'accesso privato a Google" .

Campo	Descrizione
Criterio firewall generato	Se lasci che sia la Console a generare automaticamente i criteri del firewall, devi scegliere come consentire il traffico: • Se si sceglie **Solo VPC selezionata**, il filtro di origine per il traffico in entrata è l'intervallo di subnet della VPC selezionata e l'intervallo di subnet della VPC in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le VPC**, il filtro di origine per il traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizzare i criteri firewall esistenti	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste:"Scopri le regole del firewall per Cloud Volumes ONTAP"

8. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp :
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP"
   - "Scopri come impostare le licenze"
9. **Pacchetti preconfigurati**: seleziona uno dei pacchetti per distribuire rapidamente un sistema Cloud Volumes ONTAP oppure fai clic su **Create my own configuration**. I pacchetti preconfigurati variano in base alla versione di Cloud Volumes ONTAP selezionata. Ad esempio, per Cloud Volumes ONTAP 9.18.1 e versioni successive, la Console mostra pacchetti con VM C3, inclusi dischi Hyperdisk Balanced. Puoi modificare le configurazioni, come i parametri IOPS e throughput, in base alle esigenze del tuo carico di lavoro.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.
10. **Licenze**: modifica la versione di Cloud Volumes ONTAP in base alle tue esigenze e seleziona un tipo di macchina.

    Se per una versione selezionata è disponibile una versione Release Candidate, una versione General Availability o una patch più recente, la Console aggiorna il sistema a tale versione durante la sua creazione. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.13.1 e se è disponibile la versione 9.13.1 P4. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.13 alla 9.14.
11. **Risorse di archiviazione sottostanti**: scegli le impostazioni per l'aggregato iniziale: un tipo di disco e la dimensione per ciascun disco.

    Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

    La dimensione del disco si riferisce a tutti i dischi nell'aggregato iniziale e a tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.

    Per assistenza nella scelta del tipo e della dimensione del disco, fare riferimento a"Dimensiona il tuo sistema in Google Cloud" .
12. **Cache flash, velocità di scrittura e WORM**:

a. Abilita **Flash Cache** o scegli **Normale** o **Alta** velocità di scrittura, se necessario.

   Scopri di più su "Cache flash" e "velocità di scrittura".

   > L'opzione di velocità di scrittura **Alta** offre un'elevata velocità di scrittura e un'unità di trasmissione massima (MTU) più elevata, pari a 8.896 byte. Inoltre, l'MTU più elevato di 8.896 richiede la selezione di VPC-1, VPC-2 e VPC-3 per l'implementazione. Per ulteriori informazioni su VPC-1, VPC-2 e VPC-3, fare riferimento a "Regole per VPC-1, VPC-2 e VPC-3" .

b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

   WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

"Scopri di più sullo storage WORM" .

a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.

13. **Dati in livelli in Google Cloud Platform**: scegli se abilitare i dati in livelli sull'aggregato iniziale, scegli una classe di archiviazione per i dati in livelli e quindi seleziona un account di servizio con il ruolo di amministratore di archiviazione predefinito (obbligatorio per Cloud Volumes ONTAP 9.7 o versioni successive) oppure seleziona un account Google Cloud (obbligatorio per Cloud Volumes ONTAP 9.6).

    Notare quanto segue:

    - La console imposta l'account di servizio sull'istanza di Cloud Volumes ONTAP . Questo account di servizio fornisce le autorizzazioni per il tiering dei dati in un bucket di Google Cloud Storage. Assicurati di aggiungere l'account del servizio agente della console come utente dell'account del servizio di suddivisione in livelli, altrimenti non potrai selezionarlo dalla console.
    - Per assistenza con l'aggiunta di un account Google Cloud, fare riferimento a "Configurazione e aggiunta di account Google Cloud per la suddivisione in livelli dei dati con 9.6" .
    - Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
    - Se disabiliti il data tiering, puoi abilitarlo sugli aggregati successivi, ma dovrai disattivare il sistema e aggiungere un account di servizio dal Google Cloud Console.

      "Scopri di più sulla suddivisione in livelli dei dati" .

14. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

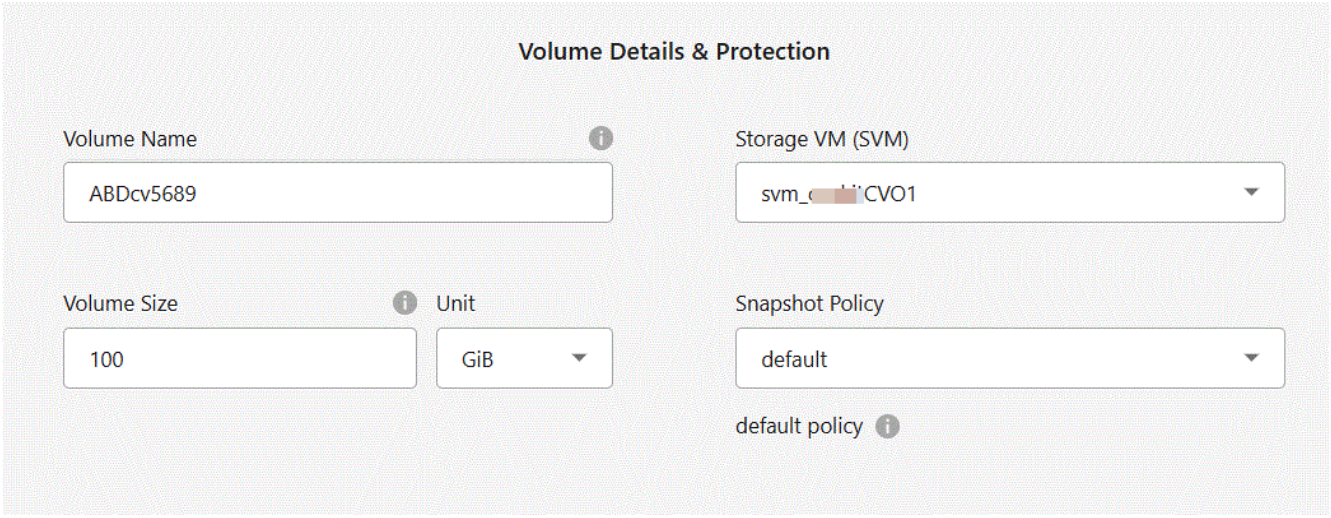
    "Scopri i protocolli e le versioni client supportati" .

    Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.

Campo	Descrizione
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



15. **Configurazione CIFS**: se hai scelto il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS. Se stai configurando Google Managed Active Directory, per impostazione predefinita puoi accedere ad AD con l'indirizzo IP 169.254.169.254.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Per configurare Google Managed Microsoft AD come server AD per Cloud Volumes ONTAP, immettere **OU=Computers,OU=Cloud** in questo campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentazione di Google Cloud: unità organizzative in Google Managed Microsoft AD"^]
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Per informazioni fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

16. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Scegli un profilo di utilizzo del volume" ,"Panoramica della suddivisione in livelli dei dati" , E "KB: Quali funzionalità di Inline Storage Efficiency sono supportate da CVO?"

17. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fai clic su **Ulteriori informazioni** per visualizzare i dettagli sul supporto e sulle risorse Google Cloud che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console distribuisce il sistema Cloud Volumes ONTAP . È possibile monitorare i progressi nella pagina **Audit**.

Se riscontri problemi durante la distribuzione del sistema Cloud Volumes ONTAP , rivedi il messaggio di errore. È anche possibile selezionare il sistema e fare clic su **Ricrea ambiente**.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

> Al termine del processo di distribuzione, non modificare le configurazioni di Cloud Volumes ONTAP generate dal sistema nel portale Google Cloud, come i tag di sistema e le etichette impostate nelle risorse Google Cloud. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdita di dati.

Avvia una coppia HA in Google Cloud

Crea un sistema nella Console per avviare Cloud Volumes ONTAP in Google Cloud.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare clic su **Archiviazione > Sistema** e seguire le istruzioni.
3. **Scegli una posizione**: seleziona **Google Cloud** e * Cloud Volumes ONTAP HA*.
4. **Dettagli e credenziali**: seleziona un progetto, specifica un nome per il cluster, seleziona facoltativamente un account di servizio, aggiungi facoltativamente delle etichette e quindi specifica le credenziali.

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Nome del sistema	La console utilizza il nome del sistema per denominare sia il sistema Cloud Volumes ONTAP sia l'istanza Google Cloud VM. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di sicurezza predefinito.
Nome dell'account di servizio	Se si prevede di utilizzare il"NetApp Cloud Tiering" O "Backup e ripristino" servizi, è necessario abilitare l'opzione **Account di servizio** e quindi selezionare l'Account di servizio che ha il ruolo di Amministratore di archiviazione predefinito.
Aggiungi etichette	Le etichette sono metadati per le tue risorse Google Cloud. La console aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse Google Cloud associate al sistema. È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un sistema, per poi aggiungerne altre dopo la creazione. Tieni presente che l'API non ti limita a quattro etichette quando crei un sistema. Per informazioni sulle etichette, fare riferimento a "Documentazione di Google Cloud: Etichettatura delle risorse" .

Campo	Descrizione
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP . È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI. Mantenere il nome utente predefinito *admin* oppure modificarlo con un nome utente personalizzato.
Modifica progetto	Seleziona il progetto in cui desideri che risieda Cloud Volumes ONTAP. Se non vedi altri progetti nell'elenco a discesa, significa che non hai ancora associato l'account di servizio ad altri progetti. Vai alla Google Cloud Console, apri il servizio IAM e seleziona il progetto. Aggiungi l'account di servizio con il ruolo che usi per la Console a quel progetto. Dovrai ripetere questo passaggio per ogni progetto. Questo è l'account di servizio che hai configurato per la Console,"come descritto in questa pagina" . Fare clic su **Aggiungi abbonamento** per associare le credenziali selezionate a un abbonamento. Per creare un sistema Cloud Volumes ONTAP con pagamento in base al consumo, è necessario selezionare un progetto Google Cloud associato a un abbonamento a Cloud Volumes ONTAP da Google Cloud Marketplace. Fare riferimento a "Associazione di un abbonamento al marketplace alle credenziali di Google Cloud" .

5. **Servizi**: seleziona i servizi che desideri utilizzare su questo sistema. Per selezionare Backup e ripristino o per utilizzare NetApp Cloud Tiering, è necessario aver specificato l'account di servizio nel passaggio 3.

   Se si desidera utilizzare WORM e il data tiering, è necessario disabilitare Backup e Recovery e distribuire un sistema Cloud Volumes ONTAP con versione 9.8 o successiva.

6. **Modelli di deployment HA**: scegli più zone (consigliato) o una singola zona per la configurazione HA. Quindi seleziona una regione e una zona.

   "Scopri di più sui modelli di distribuzione HA" .

7. **Connettività**: seleziona quattro VPC diverse per la configurazione HA, una subnet in ogni VPC, quindi scegli un criterio firewall.

   "Scopri di più sui requisiti di rete" .

   Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Politica generata	Se lasci che sia la Console a generare automaticamente i criteri del firewall, devi scegliere come consentire il traffico: • Se si sceglie **Solo VPC selezionata**, il filtro di origine per il traffico in entrata è l'intervallo di subnet della VPC selezionata e l'intervallo di subnet della VPC in cui risiede l'agente della console. Questa è l'opzione consigliata. • Se si seleziona **Tutte le VPC**, il filtro di origine per il traffico in entrata è l'intervallo IP 0.0.0.0/0.
Utilizzare esistente	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. "Scopri le regole del firewall per Cloud Volumes ONTAP" .

8. **Metodi di addebito e account NSS**: specifica quale opzione di addebito desideri utilizzare con questo sistema, quindi specifica un account del sito di supporto NetApp .
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP" .
   - "Scopri come impostare le licenze" .
9. **Pacchetti preconfigurati**: seleziona uno dei pacchetti per distribuire rapidamente un sistema Cloud Volumes ONTAP oppure fai clic su **Crea la mia configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.
10. **Licenze**: modifica la versione di Cloud Volumes ONTAP in base alle tue esigenze e seleziona un tipo di macchina.

    Se per la versione selezionata è disponibile una versione Release Candidate, una versione General Availability o una patch più recente, la Console aggiorna il sistema a tale versione durante la sua creazione. Ad esempio, l'aggiornamento avviene se si seleziona Cloud Volumes ONTAP 9.13.1 e se è disponibile la versione 9.13.1 P4. L'aggiornamento non avviene da una versione all'altra, ad esempio dalla 9.13 alla 9.14.
11. **Risorse di archiviazione sottostanti**: scegli le impostazioni per l'aggregato iniziale: un tipo di disco e la dimensione per ciascun disco.

    Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

    La dimensione del disco si riferisce a tutti i dischi nell'aggregato iniziale e a tutti gli aggregati aggiuntivi creati dalla Console quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano dimensioni del disco diverse utilizzando l'opzione di allocazione avanzata.

    Per assistenza nella scelta del tipo e della dimensione del disco, fare riferimento a"Dimensiona il tuo sistema in Google Cloud" .
12. **Cache flash, velocità di scrittura e WORM**:
    a. Abilita **Flash Cache** o scegli **Normale** o **Alta** velocità di scrittura, se necessario.

       Scopri di più su "Cache flash" e "velocità di scrittura".

Un'elevata velocità di scrittura e un'unità di trasmissione massima (MTU) più elevata di 8.896 byte sono disponibili tramite l'opzione di velocità di scrittura **Alta** con i tipi di istanza n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Inoltre, l'MTU più elevato di 8.896 richiede la selezione di VPC-1, VPC-2 e VPC-3 per l'implementazione. L'elevata velocità di scrittura e un MTU di 8.896 dipendono dalle funzionalità e non possono essere disattivati singolarmente all'interno di un'istanza configurata. Per ulteriori informazioni su VPC-1, VPC-2 e VPC-3, fare riferimento a "Regole per VPC-1, VPC-2 e VPC-3" .

b. Se lo si desidera, attivare la memorizzazione WORM (write once, read many).

WORM non può essere abilitato se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

"Scopri di più sullo storage WORM" .

a. Se si attiva l'archiviazione WORM, selezionare il periodo di conservazione.

13. **Dati a livelli in Google Cloud**: scegli se abilitare il dati a livelli nell'aggregato iniziale, scegli una classe di archiviazione per i dati a livelli e quindi seleziona un account di servizio con il ruolo di amministratore di archiviazione predefinito.

Notare quanto segue:

- La console imposta l'account di servizio sull'istanza di Cloud Volumes ONTAP . Questo account di servizio fornisce le autorizzazioni per il tiering dei dati in un bucket di Google Cloud Storage. Assicurati di aggiungere l'account del servizio agente della console come utente dell'account del servizio di suddivisione in livelli, altrimenti non potrai selezionarlo dalla console.
- Quando si crea o si modifica un volume, è possibile scegliere una specifica politica di suddivisione in livelli del volume.
- Se disabiliti il data tiering, puoi abilitarlo sugli aggregati successivi, ma dovrai disattivare il sistema e aggiungere un account di servizio dal Google Cloud Console.

"Scopri di più sulla suddivisione in livelli dei dati" .

14. **Crea volume**: inserisci i dettagli per il nuovo volume o fai clic su **Salta**.

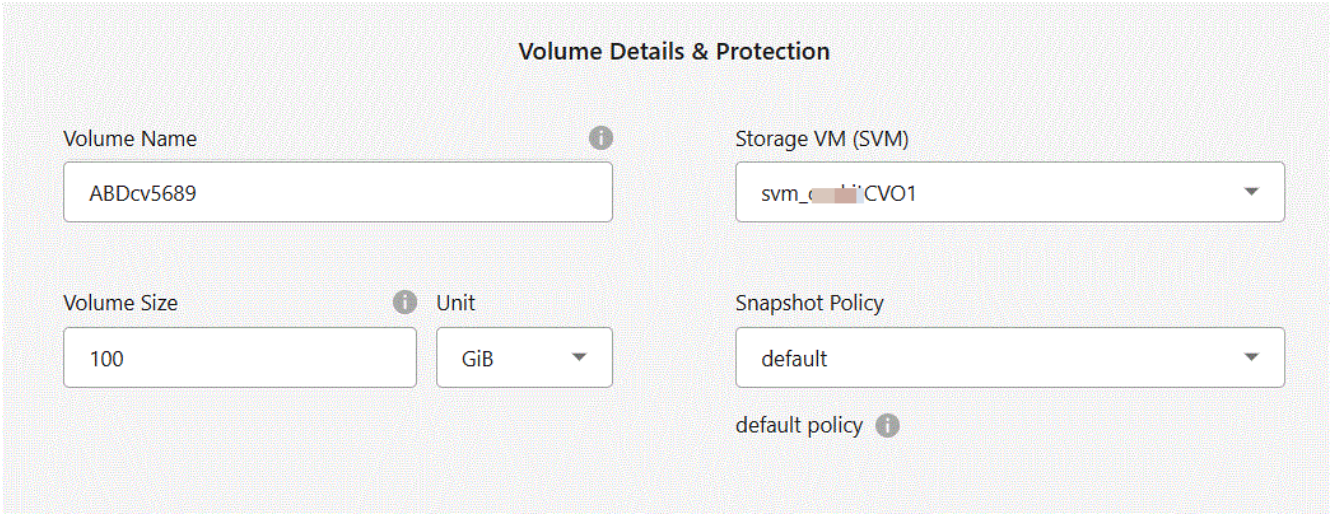
"Scopri i protocolli e le versioni client supportati" .

Alcuni campi di questa pagina sono autoesplicativi. Nella tabella seguente vengono descritti i campi per i quali potrebbe essere necessaria una guida:

Campo	Descrizione
Misurare	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.
Controllo degli accessi (solo per NFS)	Una policy di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.

Campo	Descrizione
Autorizzazioni e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Gruppo iniziatore e IQN (solo per iSCSI)	Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle di nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, quindi non è richiesta alcuna gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

L'immagine seguente mostra la prima pagina della procedura guidata per la creazione del volume:



15. **Configurazione CIFS**: se hai scelto il protocollo CIFS, configura un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS. Se stai configurando Google Managed Active Directory, per impostazione predefinita puoi accedere ad AD con l'indirizzo IP 169.254.169.254.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. Per configurare Google Managed Microsoft AD come server AD per Cloud Volumes ONTAP, immettere **OU=Computers,OU=Cloud** in questo campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentazione di Google Cloud: unità organizzative in Google Managed Microsoft AD"^]
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Server NTP	Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Fare riferimento al "Documentazione sull'automazione NetApp Console" per i dettagli. Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

16. **Profilo di utilizzo, tipo di disco e criterio di suddivisione in livelli**: scegli se abilitare le funzionalità di efficienza dell'archiviazione e modificare il criterio di suddivisione in livelli del volume, se necessario.

    Per maggiori informazioni, fare riferimento a"Scegli un profilo di utilizzo del volume" ,"Panoramica della suddivisione in livelli dei dati" , E "KB: Quali funzionalità di Inline Storage Efficiency sono supportate da CVO?"

17. **Rivedi e approva**: rivedi e conferma le tue selezioni.
    a. Esaminare i dettagli sulla configurazione.
    b. Fai clic su **Ulteriori informazioni** per visualizzare i dettagli sul supporto e sulle risorse Google Cloud che la Console acquisterà.
    c. Seleziona le caselle di controllo **Ho capito…**.
    d. Fare clic su **Vai**.

Risultato

La console distribuisce il sistema Cloud Volumes ONTAP . È possibile monitorare i progressi nella pagina **Audit**.

Se riscontri problemi durante la distribuzione del sistema Cloud Volumes ONTAP , rivedi il messaggio di errore. È anche possibile selezionare il sistema e fare clic su **Ricrea ambiente**.

Per ulteriore assistenza, vai a "Supporto NetApp Cloud Volumes ONTAP" .

Dopo aver finito

- Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare quote ai volumi, utilizzare ONTAP System Manager o ONTAP CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

> Al termine del processo di distribuzione, non modificare le configurazioni di Cloud Volumes ONTAP generate dal sistema nel portale Google Cloud, come i tag di sistema e le etichette impostate nelle risorse Google Cloud. Qualsiasi modifica apportata a queste configurazioni potrebbe causare comportamenti imprevisti o perdita di dati.

Link correlati

- "Pianificazione della configurazione Cloud Volumes ONTAP in Google Cloud"

Verifica delle immagini di Google Cloud Platform

Scopri come l'immagine di Google Cloud viene verificata in Cloud Volumes ONTAP

La verifica delle immagini di Google Cloud è conforme ai requisiti di sicurezza avanzati NetApp . Sono state apportate modifiche allo script che genera le immagini per firmare l'immagine durante il processo utilizzando chiavi private generate appositamente per questa attività. È possibile verificare l'integrità dell'immagine Google Cloud utilizzando il digest firmato e il certificato pubblico per Google Cloud, scaricabili tramite "NSS" per una versione specifica.

> La verifica delle immagini di Google Cloud è supportata dal software Cloud Volumes ONTAP versione 9.13.0 o successiva.

Converti l'immagine di Google Cloud in formato raw per Cloud Volumes ONTAP

L'immagine utilizzata per distribuire nuove istanze, aggiornamenti o utilizzata in immagini esistenti verrà condivisa con i client tramite "il sito di supporto NetApp (NSS)" . Il digest firmato e i certificati saranno disponibili per il download tramite il portale NSS. Assicurati di scaricare il digest e i certificati per la versione corretta corrispondente all'immagine condivisa dal supporto NetApp . Ad esempio, le immagini 9.13.0 avranno un digest firmato 9.13.0 e certificati disponibili su NSS.

Perché è necessario questo passaggio?

Le immagini da Google Cloud non possono essere scaricate direttamente. Per verificare l'immagine rispetto al digest firmato e ai certificati, è necessario disporre di un meccanismo per confrontare i due file e scaricare l'immagine. Per farlo, è necessario esportare/convertire l'immagine in formato disk.raw e salvare i risultati in un

bucket di archiviazione in Google Cloud. Durante il processo, il file disk.raw viene compresso con tar e gzip.

L'account utente/servizio avrà bisogno di privilegi per eseguire le seguenti operazioni:

- Accesso al bucket di archiviazione di Google
- Scrivi nel bucket di Google Storage
- Crea processi di compilazione cloud (utilizzati durante il processo di esportazione)
- Accesso all'immagine desiderata
- Crea attività di esportazione delle immagini

Per verificare l'immagine, è necessario convertirla in formato disk.raw e poi scaricarla.

Utilizza la riga di comando di Google Cloud per esportare l'immagine di Google Cloud

Il modo preferito per esportare un'immagine su Cloud Storage è utilizzare "comando di esportazione delle immagini di calcolo gcloud" . Questo comando prende l'immagine fornita e la converte in un file disk.raw che viene compresso con tar e gzip. Il file generato viene salvato nell'URL di destinazione e può quindi essere scaricato per la verifica.

Per eseguire questa operazione, l'utente/account deve disporre dei privilegi per accedere e scrivere nel bucket desiderato, esportare l'immagine e creare build cloud (utilizzate da Google per esportare l'immagine).

Esporta l'immagine di Google Cloud utilizzando gcloud

Clicca per visualizzare

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

Estrarre i file compressi

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Per ulteriori informazioni su come esportare un'immagine tramite Google Cloud, fare riferimento a "Documento di Google Cloud sull'esportazione di un'immagine" .

Verifica della firma dell'immagine

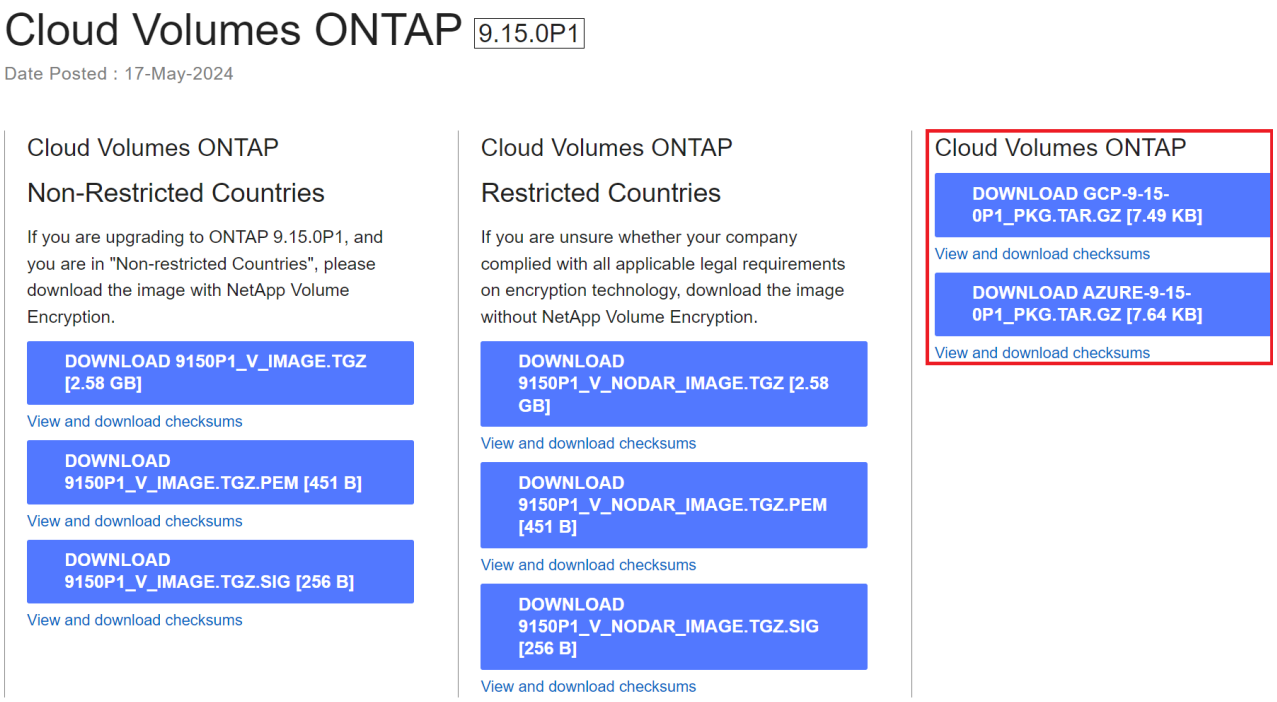
Verifica della firma dell'immagine di Google Cloud per Cloud Volumes ONTAP

Per verificare l'immagine firmata da Google Cloud esportata, è necessario scaricare il file digest dell'immagine dall'NSS per convalidare il file disk.raw e il contenuto del file digest.

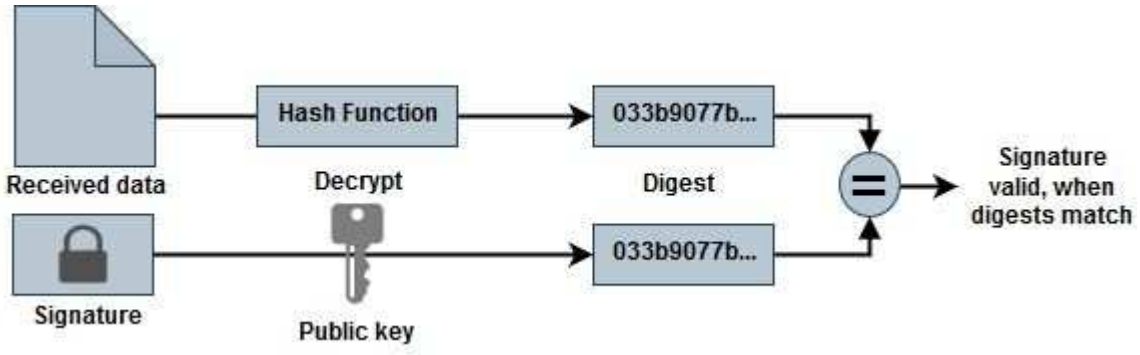
Riepilogo del flusso di lavoro di verifica delle immagini firmate

Di seguito è riportata una panoramica del processo di verifica delle immagini firmate di Google Cloud.

- Dal "NSS" , scarica l'archivio Google Cloud contenente i seguenti file:
  - Digest firmato (.sig)
  - Certificato contenente la chiave pubblica (.pem)
  - Catena di certificati (.pem)



- Scarica il file disk.raw convertito
- Convalidare il certificato utilizzando la catena di certificati
- Convalida il digest firmato utilizzando il certificato che contiene la chiave pubblica
  - Decrittografare il digest firmato utilizzando la chiave pubblica per estrarre il digest del file immagine
  - Crea un digest del file disk.raw scaricato
  - Confronta i due file digest per la convalida



Verificare il file disk.raw dell'immagine di Google Cloud per Cloud Volumes ONTAP utilizzando OpenSSL

È possibile verificare il file disk.raw scaricato da Google Cloud rispetto al contenuto del file digest disponibile tramite "NSS" utilizzando OpenSSL.

I comandi OpenSSL per convalidare l'immagine sono compatibili con i computer Linux, macOS e Windows.

Passi

1. Verificare il certificato utilizzando OpenSSL.

Clicca per visualizzare

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
         e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
         22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
         38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
         fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
         bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Posizionare il file disk.raw scaricato, la firma e i certificati in una directory.
3. Estrarre la chiave pubblica dal certificato utilizzando OpenSSL.
4. Decifrare la firma utilizzando la chiave pubblica estratta e verificare il contenuto del file disk.raw scaricato.

Clicca per visualizzare

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Utilizzare Cloud Volumes ONTAP

Gestione delle licenze

Gestisci le licenze basate sulla capacità per Cloud Volumes ONTAP

Gestisci le tue licenze basate sulla capacità dalla NetApp Console per assicurarti che il tuo account NetApp disponga di capacità sufficiente per i tuoi sistemi Cloud Volumes ONTAP .

Le *licenze basate sulla capacità* consentono di pagare Cloud Volumes ONTAP per TiB di capacità.

È possibile gestire le licenze Cloud Volumes ONTAP basate sulla capacità dalla NetApp Console.

> Sebbene l'utilizzo effettivo e la misurazione dei prodotti e dei servizi gestiti nella Console siano sempre calcolati in GiB e TiB, i termini GB/GiB e TB/TiB vengono utilizzati in modo intercambiabile. Ciò si riflette negli elenchi di Cloud Marketplace, nei preventivi di prezzo, nelle descrizioni degli elenchi e in altra documentazione di supporto

"Scopri di più sulle licenze Cloud Volumes ONTAP" .

Come vengono aggiunte le licenze alla NetApp Console

Dopo aver acquistato una licenza dal tuo rappresentante commerciale NetApp , NetApp ti invierà un'e-mail con il numero di serie e ulteriori dettagli sulla licenza.

Nel frattempo, la Console interroga automaticamente il servizio licenze di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. Se non ci sono errori, aggiunge le licenze.

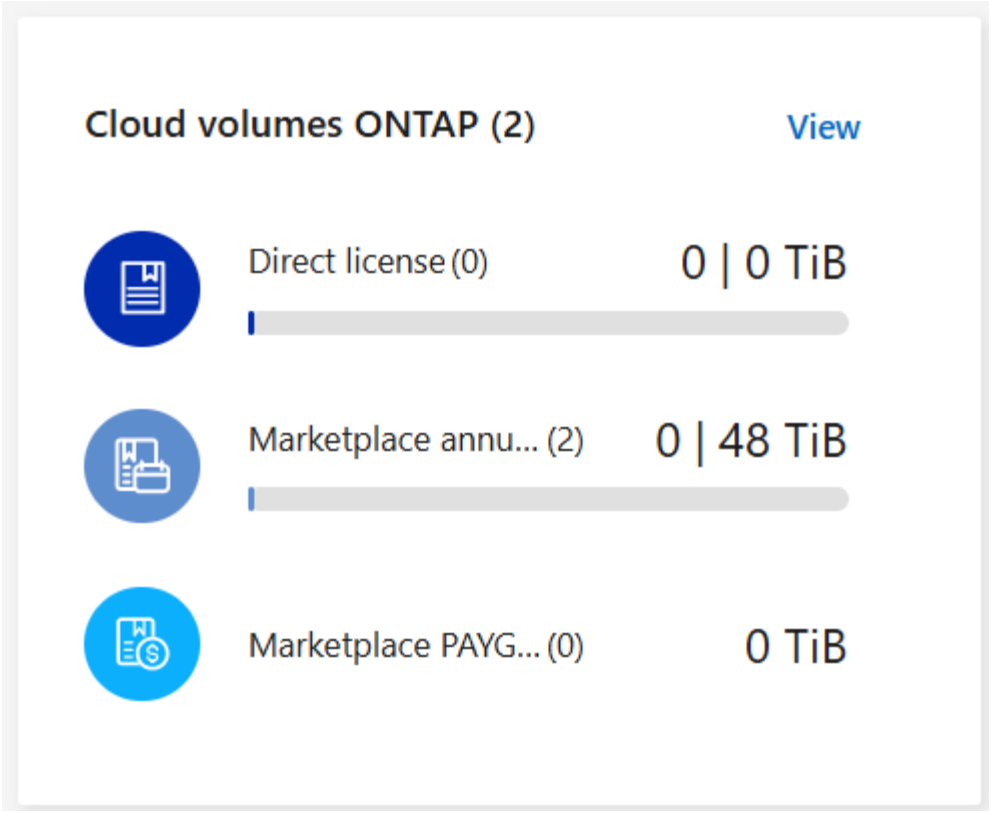
Se la Console non riesce ad aggiungere la licenza, sarà necessario aggiungerla manualmente. Ad esempio, se l'agente Console è installato in una posizione che non dispone di accesso a Internet, sarà necessario aggiungere le licenze manualmente. "Scopri come aggiungere le licenze acquistate al tuo account" .

Visualizza la capacità consumata nel tuo account

La Console mostra la capacità totale consumata nel tuo account e la capacità consumata per pacchetto di licenza. Questo può aiutarti a capire come ti vengono addebitati i costi e se devi acquistare capacità aggiuntiva.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Nella scheda **Panoramica**, il riquadro Cloud Volumes ONTAP mostra la capacità corrente fornita per il tuo account.



- La *licenza diretta* è la capacità totale fornita di tutti i sistemi Cloud Volumes ONTAP nel tuo account NetApp . La tariffazione si basa sulla dimensione di ciascun volume, indipendentemente dallo spazio locale, utilizzato, archiviato o effettivo all'interno del volume.
- Il *contratto annuale* è la capacità totale concessa in licenza (Bring Your Own License (BYOL) o contratto Marketplace) acquistata da NetApp.
- *PAYGO* è la capacità totale fornita utilizzando gli abbonamenti al cloud marketplace. La ricarica tramite PAYGO viene utilizzata solo se la capacità consumata è superiore alla capacità concessa in licenza o se nella Console non è disponibile alcuna licenza BYOL.

3. Selezionare **Visualizza** per visualizzare la capacità utilizzata per ciascuno dei pacchetti di licenza.
4. Seleziona la scheda **Licenze** per visualizzare i dettagli di ogni licenza del pacchetto che hai acquistato.

   Per comprendere meglio le capacità visualizzate nel pacchetto Essentials, è necessario avere familiarità con il funzionamento della ricarica. "Scopri come addebitare il pacchetto Essentials" .

5. Selezionare la scheda **Abbonamenti** per visualizzare la capacità consumata in base al modello di consumo delle licenze. Questa scheda include sia le licenze PAYGO che quelle con contratto annuale.

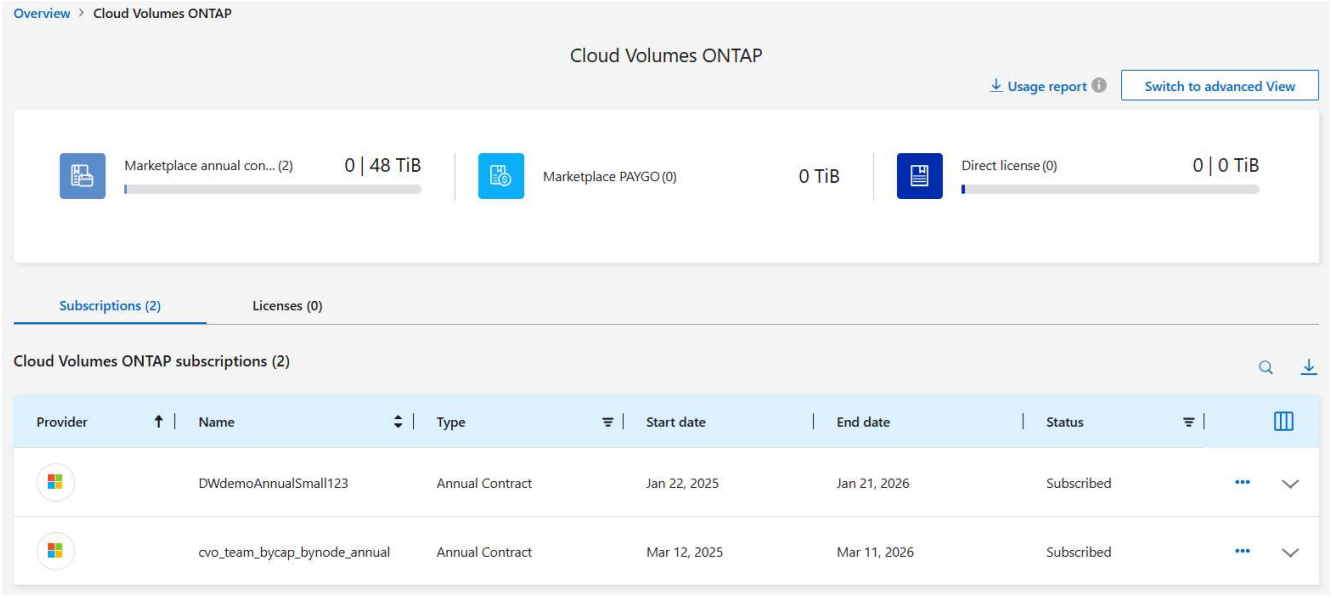
   Vedrai solo gli abbonamenti associati all'organizzazione che stai visualizzando in quel momento.

6. Mentre visualizzi le informazioni sui tuoi abbonamenti, puoi interagire con i dettagli nella tabella. Espandi una riga per visualizzare maggiori dettagli.
   - Selezionare per scegliere quali colonne visualizzare nella tabella. Si noti che le colonne Termine e Rinnovo automatico non vengono visualizzate per impostazione predefinita. La colonna Rinnovo automatico visualizza le informazioni sul rinnovo solo per i contratti Azure.

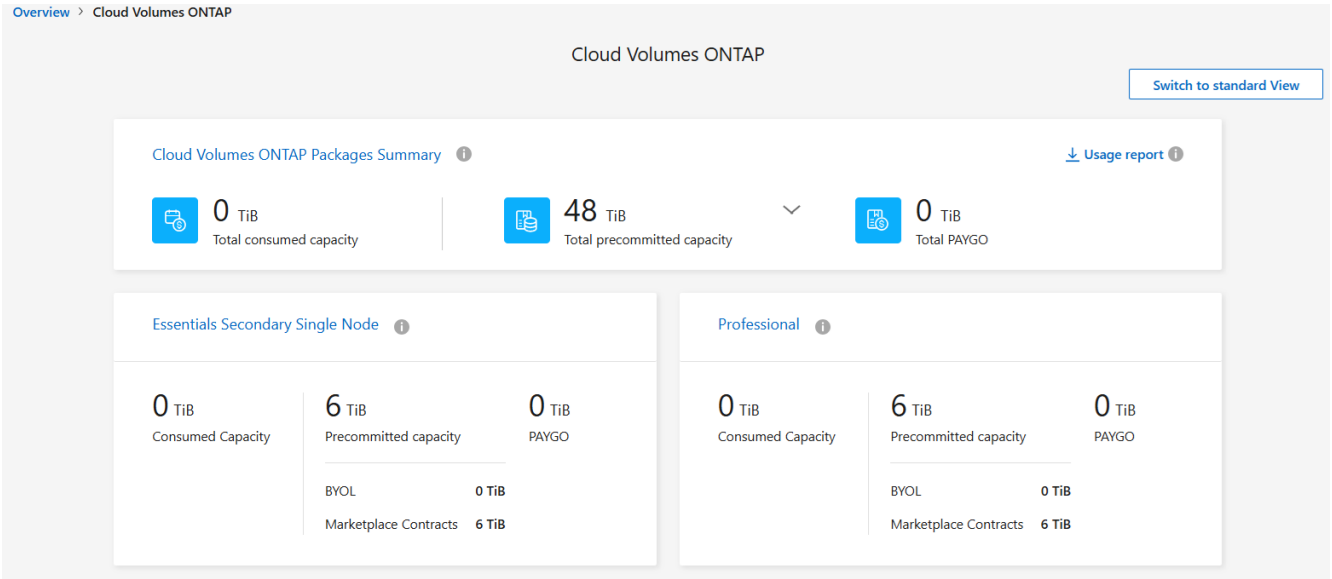
Visualizzazione dei dettagli del pacchetto

È possibile visualizzare i dettagli sulla capacità utilizzata per pacchetto passando alla modalità legacy nella pagina Cloud Volumes ONTAP .

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Nella scheda **Panoramica**, il riquadro Cloud Volumes ONTAP mostra la capacità corrente fornita per il tuo account.
3. Selezionare **Visualizza** per visualizzare la capacità fornita per ciascuno dei pacchetti di licenza.
4. Seleziona **Passa alla visualizzazione avanzata**.



5. Visualizza i dettagli del pacchetto che desideri vedere.



Cambia metodo di addebito

La licenza basata sulla capacità è disponibile sotto forma di *pacchetto*. Quando si crea un sistema Cloud Volumes ONTAP , è possibile scegliere tra diversi pacchetti di licenze in base alle esigenze aziendali. Se le tue

esigenze cambiano dopo aver creato il sistema, puoi cambiare il pacchetto in qualsiasi momento. Ad esempio, potresti passare dal pacchetto Essentials al pacchetto Professional.

"Scopri di più sui pacchetti di licenze basati sulla capacità" .

Informazioni su questo compito

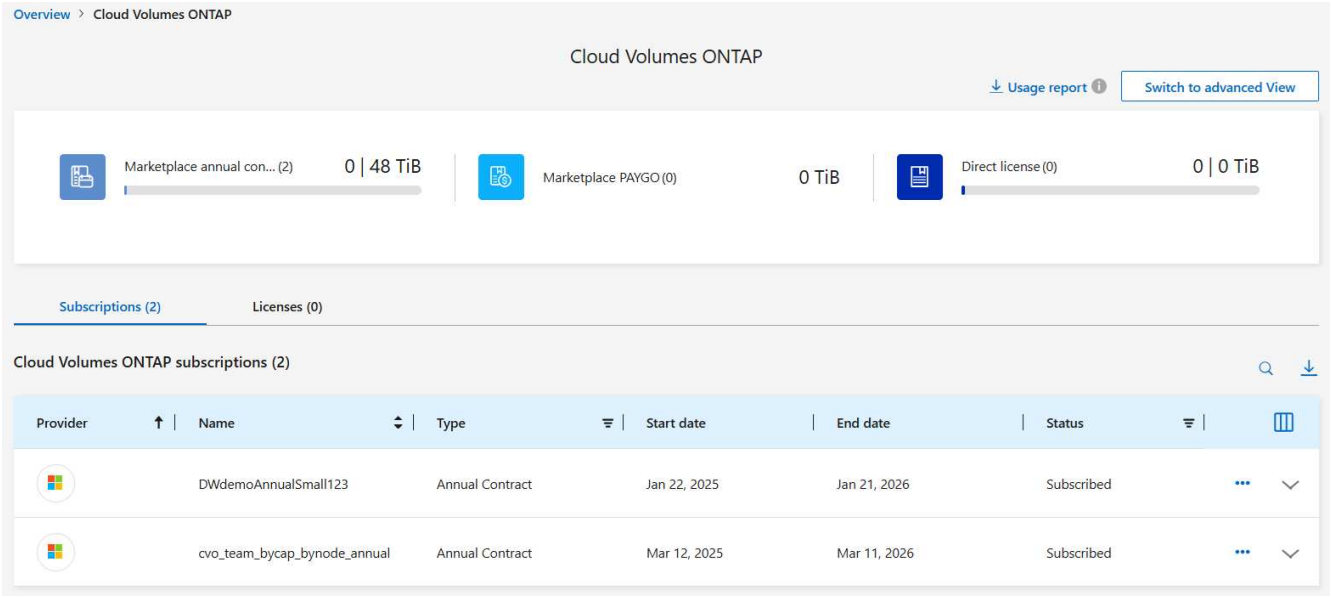
- La modifica del metodo di addebito non influisce sul fatto che l'addebito avvenga tramite una licenza acquistata da NetApp (BYOL) o tramite l'abbonamento pay-as-you-go (PAYGO) del marketplace del tuo provider cloud.

  La console tenta sempre di addebitare prima una licenza. Se una licenza non è disponibile, verrà addebitato un abbonamento al marketplace. Non è necessario convertire un abbonamento BYOL in un abbonamento Marketplace o viceversa.

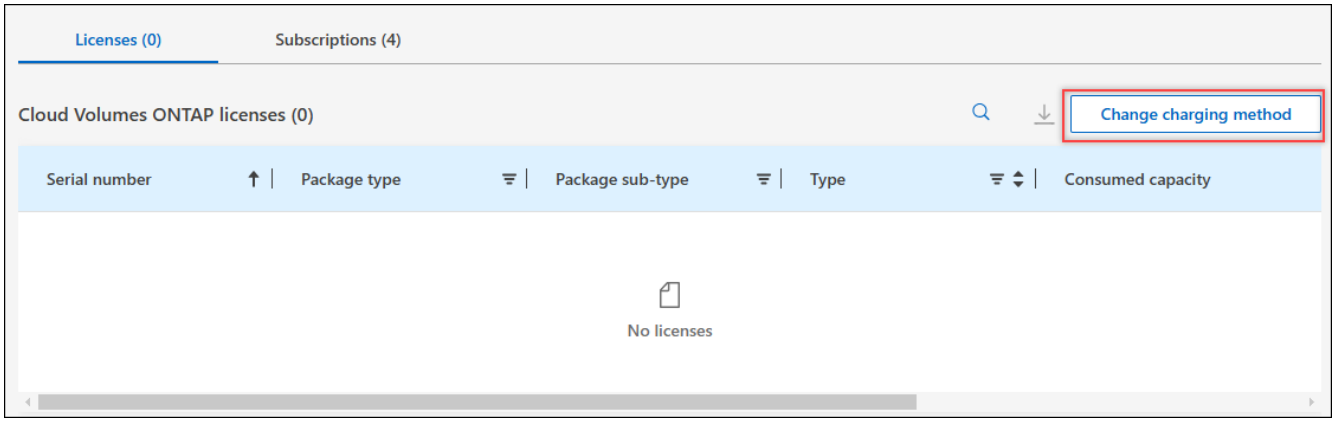
- Se hai un'offerta o un contratto privato dal marketplace del tuo provider cloud, il passaggio a un metodo di addebito non incluso nel contratto comporterà l'addebito di BYOL (se hai acquistato una licenza da NetApp) o PAYGO.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Seleziona **Passa alla visualizzazione avanzata**.



5. Scorrere verso il basso fino alla tabella **Licenza basata sulla capacità** e selezionare **Cambia metodo di addebito**.



6. Nel pop-up **Cambia metodo di addebito**, seleziona un sistema Cloud Volumes ONTAP , scegli il nuovo metodo di addebito e conferma di aver compreso che la modifica del tipo di pacchetto inciderà sui costi del servizio.
7. Seleziona **Cambia metodo di addebito**.

Scarica i report di utilizzo

È possibile scaricare quattro report di utilizzo dalla Console. Questi report sull'utilizzo forniscono dettagli sulla capacità dei tuoi abbonamenti e ti indicano come ti vengono addebitate le risorse nei tuoi abbonamenti Cloud Volumes ONTAP . I report scaricabili acquisiscono i dati in un dato momento e possono essere facilmente condivisi con altri.

I seguenti report sono disponibili per il download. I valori di capacità indicati sono in TiB.

- **Utilizzo di alto livello**: questo report include le seguenti informazioni:
  - Capacità totale consumata
  - Capacità preimpegnata totale
  - Capacità BYOL totale
  - Capacità totale dei contratti del Marketplace
  - Capacità PAYGO totale
- * Utilizzo del pacchetto Cloud Volumes ONTAP *: questo report include le seguenti informazioni per ciascun pacchetto:
  - Capacità totale consumata
  - Capacità preimpegnata totale
  - Capacità BYOL totale
  - Capacità totale dei contratti del Marketplace
  - Capacità PAYGO totale
- **Utilizzo delle VM di storage**: questo report mostra come la capacità addebitata viene suddivisa tra i

sistemi Cloud Volumes ONTAP e le macchine virtuali di storage (SVM). Questa informazione è disponibile solo nel rapporto. Contiene le seguenti informazioni:

- ID e nome del sistema (appare come UUID)
- Nuvola
- ID account NetApp
- Configurazione del sistema
- Nome SVM
- Capacità fornita
- Riepilogo della capacità carica
- Termini di fatturazione del Marketplace
- Pacchetto o funzionalità Cloud Volumes ONTAP
- Nome dell'abbonamento al Marketplace SaaS di addebito
- ID abbonamento SaaS Marketplace di addebito
- Tipo di carico di lavoro

- **Utilizzo dei volumi**: questo report mostra come la capacità addebitata viene suddivisa in base ai volumi in un sistema Cloud Volumes ONTAP . Questa informazione non è disponibile in nessuna schermata della Console. Include le seguenti informazioni:
  - ID e nome del sistema (appare come UUID)
  - Nome SVN
  - ID volume
  - Tipo di volume
  - Capacità fornita in volume

> I volumi FlexClone non sono inclusi in questo report perché questi tipi di volumi non comportano costi.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Nella scheda **Panoramica**, seleziona **Visualizza** dal riquadro Cloud Volumes ONTAP .
3. Selezionare **Report di utilizzo**.

   Il report di utilizzo viene scaricato.

4. Aprire il file scaricato per accedere ai report.

Gestisci gli abbonamenti Keystone per Cloud Volumes ONTAP tramite NetApp Console

Gestisci i tuoi abbonamenti Keystone nella NetApp Console abilitando gli abbonamenti per l'uso con Cloud Volumes ONTAP e richiedendo modifiche alla capacità impegnata per i livelli di servizio del tuo abbonamento. Richiedendo capacità aggiuntiva per un livello di servizio si ottiene più spazio di archiviazione per i sistemi Cloud Volumes ONTAP .

NetApp Keystone è un servizio flessibile basato su abbonamento con pagamento in base alla crescita che offre un'esperienza cloud ibrida ai clienti che preferiscono OpEx a CapEx o leasing.

"Scopri di più su Keystone"

Autorizza il tuo account

Prima di poter utilizzare e gestire gli abbonamenti Keystone nella Console, è necessario contattare NetApp per autorizzare l'account Console con gli abbonamenti Keystone .

Passi

1. Dal menu NetApp Console , selezionare **Amministrazione > Licenses and subscriptions**.
2. Seleziona *Abbonamenti Keystone *.
3. Se vedi la pagina **Benvenuti in NetApp Keystone**, invia un'e-mail all'indirizzo indicato nella pagina.

   Un rappresentante NetApp elaborerà la tua richiesta autorizzando il tuo account ad accedere agli abbonamenti.

4. Torna alla scheda *Abbonamenti Keystone * per visualizzare i tuoi abbonamenti.

Collega un abbonamento

Dopo che NetApp avrà autorizzato il tuo account, potrai collegare gli abbonamenti Keystone per utilizzarli con Cloud Volumes ONTAP. Questa azione consente agli utenti di selezionare l'abbonamento come metodo di addebito per i nuovi sistemi Cloud Volumes ONTAP .

Passi

1. Dal menu NetApp Console , selezionare **Amministrazione > Licenses and subscriptions**.
2. Seleziona *Abbonamenti Keystone *.
3. Per l'abbonamento che vuoi collegare, clicca ••• e seleziona **Collegamento**.

Risultato

L'abbonamento è ora collegato all'organizzazione o all'account della console e può essere selezionato durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP .

Richiedi più o meno capacità impegnata

Se desideri modificare la capacità impegnata per i livelli di servizio del tuo abbonamento, puoi inviare una richiesta a NetApp direttamente dalla Console. Richiedendo capacità aggiuntiva per un livello di servizio si ottiene più spazio di archiviazione per i sistemi Cloud Volumes ONTAP .

Passi

1. Dal menu NetApp Console , selezionare **Amministrazione > Licenses and subscriptions**.
2. Seleziona *Abbonamenti Keystone *.
3. Per l'abbonamento di cui si desidera regolare la capacità, fare clic su ••• e seleziona **Visualizza dettagli e modifica**.
4. Inserisci la capacità impegnata richiesta per uno o più abbonamenti.
5. Scorri verso il basso, inserisci eventuali dettagli aggiuntivi per la richiesta, quindi fai clic su **Invia**.

Risultato

La tua richiesta crea un ticket nel sistema NetApp per l'elaborazione.

Monitorare l'utilizzo

La dashboard Digital Advisor consente di monitorare l'utilizzo dell'abbonamento Keystone e di generare report.

"Scopri di più sul monitoraggio dell'utilizzo degli abbonamenti"

Scollegare un abbonamento

Se non desideri più utilizzare un abbonamento Keystone con la Console, puoi scollegarlo. Tieni presente che puoi scollegare solo un abbonamento che non è collegato a un abbonamento Cloud Volumes ONTAP esistente.

Passi

1. Dal menu NetApp Console , selezionare **Amministrazione > Licenses and subscriptions**.
2. Seleziona * Keystone*.
3. Per l'abbonamento che vuoi scollegare, clicca ••• e seleziona **Scollega**.

Risultato

L'abbonamento è scollegato dall'organizzazione o dall'account della Console e non è più disponibile per la selezione durante la creazione di un ambiente di lavoro Cloud Volumes ONTAP .

Gestisci le licenze basate sui nodi per Cloud Volumes ONTAP

Gestire le licenze basate sui nodi nella NetApp Console per garantire che ogni sistema Cloud Volumes ONTAP disponga di una licenza valida con la capacità richiesta.

Le *licenze basate su nodi* rappresentano il modello di licenza della generazione precedente (e non sono disponibili per i nuovi clienti):

- Licenze BYOL (Bring Your Own License) acquistate da NetApp
- Abbonamenti orari a consumo (PAYGO) dal marketplace del tuo provider cloud

È possibile gestire le licenze Cloud Volumes ONTAP basate su nodi dalla NetApp Console.

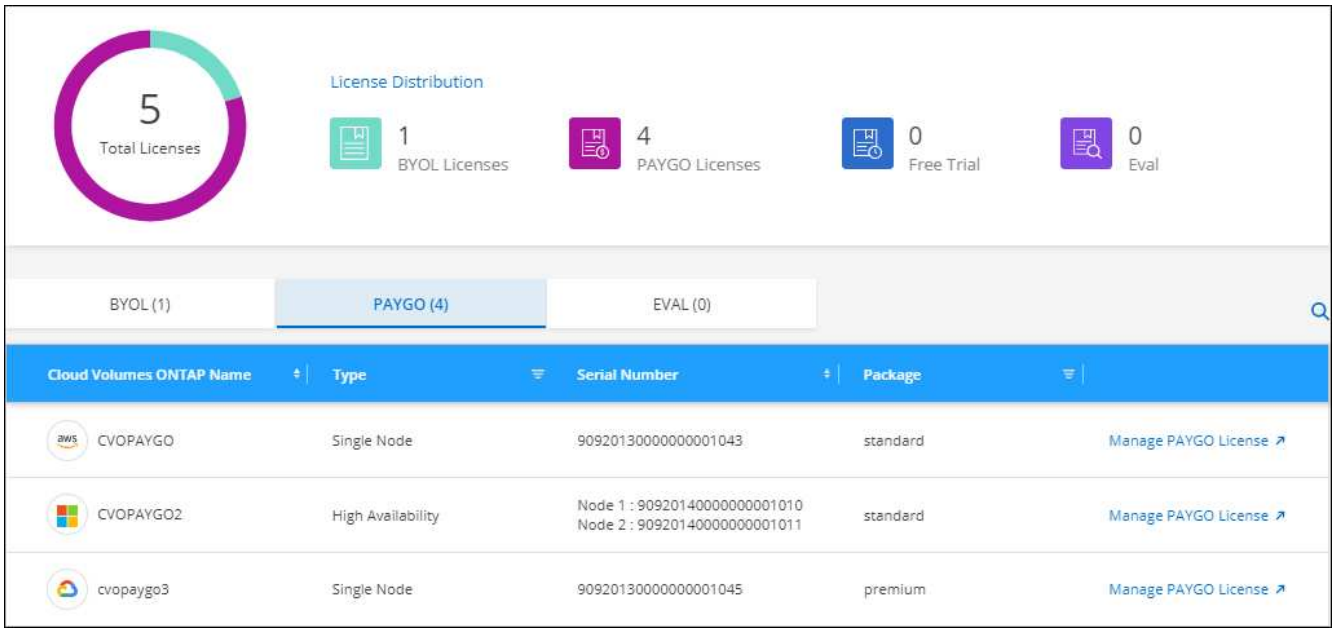
"Scopri di più sulle licenze Cloud Volumes ONTAP" .

Gestire le licenze PAYGO

Il menu Licenses and subscriptions consente di visualizzare i dettagli su ciascuno dei sistemi PAYGO Cloud Volumes ONTAP , tra cui il numero di serie e il tipo di licenza PAYGO.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Selezionare **Licenze basate su nodi** dal menu a discesa.
5. Fare clic su **PAYGO**.
6. Visualizza i dettagli nella tabella per ciascuna delle tue licenze PAYGO.



7. Se necessario, fare clic su **Gestisci licenza PAYGO** per modificare la licenza PAYGO o per modificare il tipo di istanza.

Gestire le licenze BYOL

Gestisci le licenze acquistate direttamente da NetApp aggiungendo e rimuovendo licenze di sistema e licenze di capacità extra.

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

Aggiungi licenze non assegnate

Aggiungere una licenza basata su nodi alla Console in modo da poter selezionare la licenza quando si crea un nuovo sistema Cloud Volumes ONTAP . La Console identifica queste licenze come *non assegnate*.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Selezionare **Licenze basate su nodi** dal menu a discesa.
5. Fare clic su **Non assegnato**.
6. Fare clic su **Aggiungi licenze non assegnate**.
7. Inserisci il numero di serie della licenza o carica il file della licenza.

   Se non si dispone ancora del file di licenza, fare riferimento alla sezione seguente.

8. Fare clic su **Aggiungi licenza**.

Risultato

La console aggiunge la licenza. La licenza verrà identificata come non assegnata finché non la assocerai a un nuovo sistema Cloud Volumes ONTAP . Dopodiché la licenza viene spostata nella scheda **BYOL** in * Licenses

and subscriptions*.

Scambia licenze basate su nodi non assegnati

Se disponi di una licenza basata su nodi non assegnata per Cloud Volumes ONTAP che non hai utilizzato, puoi scambiare la licenza convertendola in una licenza NetApp Backup and Recovery , una licenza NetApp Data Classification o una licenza NetApp Cloud Tiering .

Lo scambio della licenza revoca la licenza Cloud Volumes ONTAP e crea una licenza equivalente in dollari per il servizio:

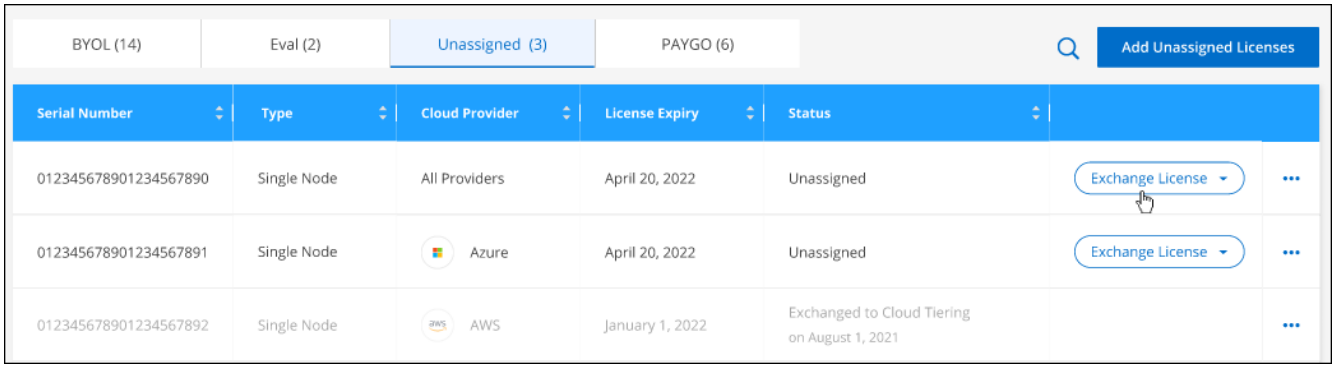
- La licenza per una coppia Cloud Volumes ONTAP HA viene convertita in una licenza diretta da 51 TiB
- La licenza per un singolo nodo Cloud Volumes ONTAP viene convertita in una licenza diretta da 32 TiB

La licenza convertita ha la stessa data di scadenza della licenza Cloud Volumes ONTAP .

"Visualizza la procedura dettagliata su come scambiare licenze basate su nodi."

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Selezionare **Licenze basate su nodi** dal menu a discesa.
5. Fare clic su **Non assegnato**.
6. Fare clic su **Scambia licenza**.



7. Seleziona il servizio con cui desideri scambiare la licenza.
8. Se richiesto, selezionare una licenza aggiuntiva per la coppia HA.
9. Leggi il consenso legale e clicca su **Accetto**.

Risultato

La Console converte la licenza non assegnata nel servizio selezionato. È possibile visualizzare la nuova licenza nella scheda **Licenze servizi dati**.

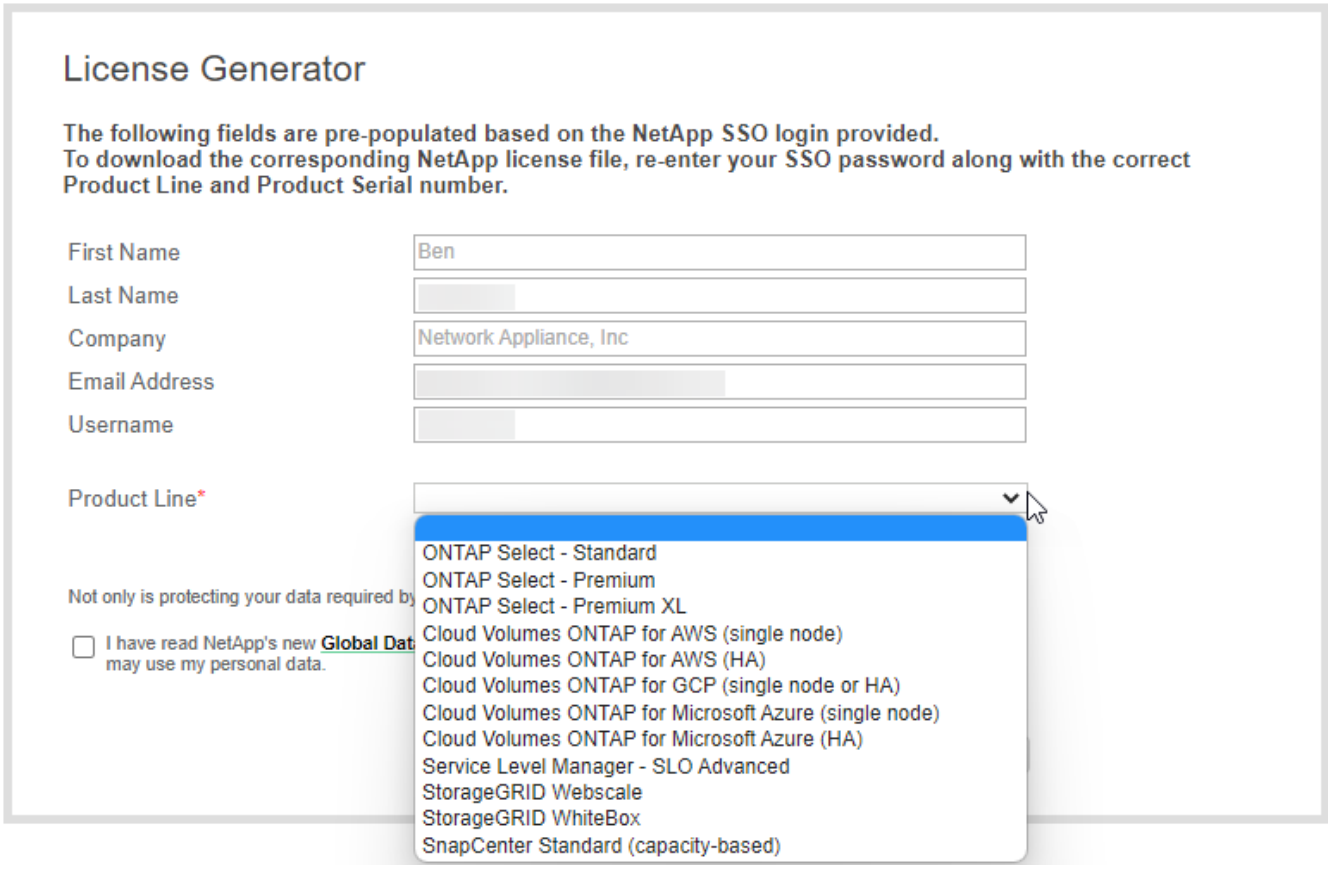
Ottenere un file di licenza di sistema

Nella maggior parte dei casi, la Console può ottenere automaticamente il file di licenza tramite l'account del sito di supporto NetApp . In caso contrario, sarà necessario caricare manualmente il file di licenza. Se non si dispone del file di licenza, è possibile ottenerlo da netapp.com.

Passi

1. Vai al "Generatore di file di licenza NetApp" e accedi utilizzando le credenziali del sito di supporto NetApp .
2. Inserisci la tua password, scegli il tuo prodotto, inserisci il numero di serie, conferma di aver letto e accettato l'informativa sulla privacy, quindi clicca su **Invia**.

   Esempio



3. Scegli se desideri ricevere il file JSON serialnumber.NLF tramite e-mail o tramite download diretto.

Aggiornare una licenza di sistema

Quando si rinnova un abbonamento BYOL contattando un rappresentante NetApp , la Console ottiene automaticamente la nuova licenza da NetApp e la installa sul sistema Cloud Volumes ONTAP . Se la Console non riesce ad accedere al file di licenza tramite la connessione Internet protetta, puoi ottenere il file autonomamente e poi caricarlo manualmente.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Selezionare **Licenze basate su nodi** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli per un sistema Cloud Volumes ONTAP .
6. Fare clic sul menu azioni accanto alla licenza di sistema e selezionare **Aggiorna licenza**.
7. Carica il file di licenza (o i file se hai una coppia HA).

8. Fare clic su **Aggiorna licenza**.

Risultato

La console aggiorna la licenza sul sistema Cloud Volumes ONTAP .

Gestisci le licenze di capacità extra

È possibile acquistare licenze di capacità extra per un sistema Cloud Volumes ONTAP BYOL per allocare una capacità superiore ai 368 TiB forniti con una licenza di sistema BYOL. Ad esempio, potresti acquistare una licenza di capacità aggiuntiva per allocare fino a 736 TiB di capacità a Cloud Volumes ONTAP. Oppure puoi acquistare tre licenze di capacità extra per arrivare fino a 1,4 PiB.

Il numero di licenze che è possibile acquistare per un sistema a nodo singolo o una coppia HA è illimitato.

Aggiungi licenze di capacità

Acquista una licenza con capacità extra contattandoci tramite l'icona della chat in basso a destra della Console. Dopo aver acquistato la licenza, è possibile applicarla a un sistema Cloud Volumes ONTAP .

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Selezionare **Licenze basate su nodi** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli per un sistema Cloud Volumes ONTAP .
6. Fare clic su **Aggiungi licenza di capacità**.
7. Inserisci il numero di serie o carica il file di licenza (o i file se hai una coppia HA).
8. Fare clic su **Aggiungi licenza di capacità**.

Aggiorna le licenze di capacità

Se hai esteso la durata di una licenza con capacità extra, dovrai aggiornare la licenza nella Console.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Selezionare **Licenze basate su nodi** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli per un sistema Cloud Volumes ONTAP .
6. Fare clic sul menu azioni accanto alla licenza di capacità e selezionare **Aggiorna licenza**.
7. Carica il file di licenza (o i file se hai una coppia HA).
8. Fare clic su **Aggiorna licenza**.

Rimuovere le licenze di capacità

Se una licenza con capacità extra è scaduta e non è più in uso, è possibile rimuoverla in qualsiasi momento.

Passi

1. Dal riquadro di navigazione a sinistra, seleziona **Amministrazione > Licenses and subscriptions**.
2. Selezionare la scheda **Panoramica**.
3. Nel riquadro Cloud Volumes ONTAP , seleziona **Visualizza**.
4. Selezionare **Licenze basate su nodi** dal menu a discesa.
5. Nella scheda **BYOL**, espandere i dettagli per un sistema Cloud Volumes ONTAP .
6. Fare clic sul menu azioni accanto alla licenza di capacità e selezionare **Rimuovi licenza**.
7. Fare clic su **Rimuovi**.

Cambiamento tra PAYGO e BYOL

La conversione di un sistema da una licenza PAYGO per nodo a una licenza BYOL per nodo (e viceversa) non è supportata. Se si desidera passare da un abbonamento pay-as-you-go a un abbonamento BYOL, è necessario implementare un nuovo sistema e replicare i dati dal sistema esistente al nuovo sistema.

Passi

1. Creare un nuovo sistema Cloud Volumes ONTAP .
2. Impostare una replica dei dati una tantum tra i sistemi per ogni volume che si desidera replicare.

   "Scopri come replicare i dati tra i sistemi"

3. Terminare il sistema Cloud Volumes ONTAP di cui non si ha più bisogno eliminando il sistema originale.

   "Scopri come eliminare un sistema Cloud Volumes ONTAP" .

Link correlati

collegamento:"Fine della disponibilità delle licenze basate sui nodi" "Convertire le licenze basate sui nodi in licenze basate sulla capacità"

Amministrazione del volume e LUN

Creare un FlexVol volume su un sistema Cloud Volumes ONTAP

Se hai bisogno di più spazio di archiviazione dopo aver avviato il tuo sistema Cloud Volumes ONTAP iniziale, puoi creare nuovi volumi FlexVol per NFS, CIFS o iSCSI dalla NetApp Console.

Esistono diversi modi per creare un nuovo volume:

- Specifica i dettagli per un nuovo volume e lascia che la Console gestisca per te gli aggregati di dati sottostanti.Saperne di più
- Crea un volume su un aggregato di dati a tua scelta.Saperne di più
- Creare un volume sul secondo nodo in una configurazione HA.Saperne di più

Prima di iniziare

Alcune note sul provisioning dei volumi:

- Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto

creando una sola LUN per volume, eliminando così ogni attività di gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

- È possibile creare LUN aggiuntivi da ONTAP System Manager o da ONTAP CLI.
- Se si desidera utilizzare CIFS in AWS, è necessario aver configurato DNS e Active Directory. Per i dettagli, fare riferimento a"Requisiti di rete per Cloud Volumes ONTAP per AWS" .
- Se la configurazione Cloud Volumes ONTAP supporta la funzionalità Amazon EBS Elastic Volumes, potrebbe essere necessario"scopri di più su cosa succede quando crei un volume" .

Crea un volume

Il modo più comune per creare un volume è specificare il tipo di volume necessario e poi lasciare che la Console gestisca l'allocazione del disco per te. Ma hai anche la possibilità di scegliere l'aggregato specifico su cui vuoi creare il volume.

Passi

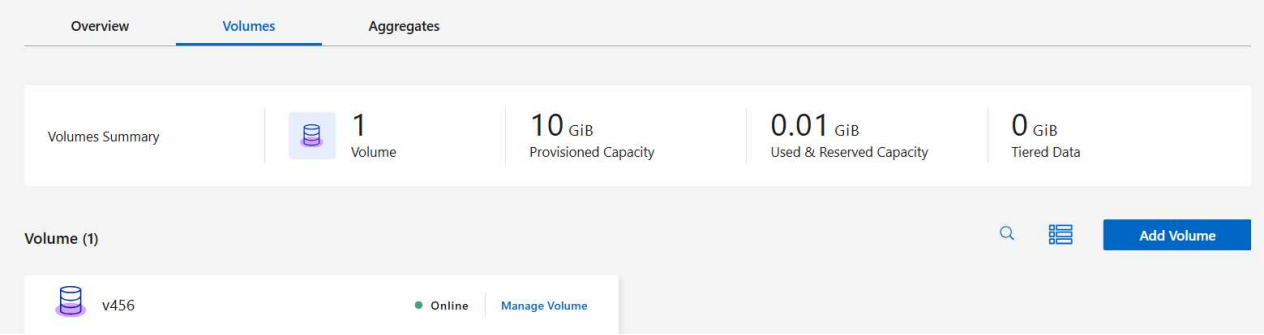
1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema Cloud Volumes ONTAP su cui si desidera effettuare il provisioning di un FlexVol volume.

   È possibile creare un volume lasciando che la Console gestisca l'allocazione del disco per conto dell'utente oppure scegliere un aggregato specifico per il volume. Si consiglia di scegliere un aggregato specifico solo se si ha una buona conoscenza degli aggregati di dati sul sistema Cloud Volumes ONTAP .

Qualsiasi aggregato

Selezionare la scheda Volumi e fare clic su **Aggiungi volume**

.

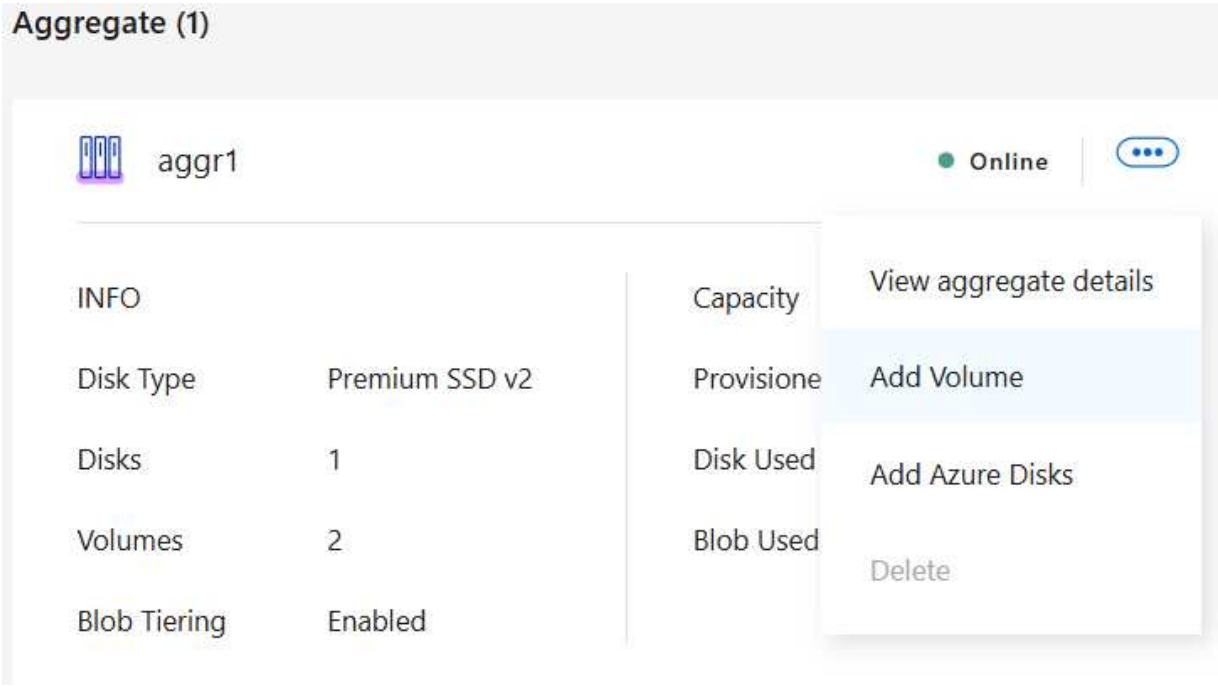


Aggregato specifico

a. Nella scheda **Aggregati**, vai all'aggregato richiesto e fai clic su ••• icona.

b. Selezionare **Aggiungi volume**

.



3. Seguire i passaggi della procedura guidata per creare il volume.

   a. **Dettagli, protezione e tag**: immettere i dettagli di base sul volume e selezionare un criterio Snapshot.

      Alcuni campi di questa pagina sono autoesplicativi. L'elenco seguente descrive i campi per i quali potresti aver bisogno di assistenza:

Campo	Descrizione
Nome del volume	Il nome identificabile che puoi immettere per il nuovo volume.

Campo	Descrizione
Dimensione del volume	La dimensione massima che è possibile immettere dipende in larga misura dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello spazio di archiviazione fisico attualmente disponibile.
VM di archiviazione (SVM)	Una VM di archiviazione è una macchina virtuale in esecuzione all'interno di ONTAP che fornisce servizi di archiviazione e dati ai tuoi client. Potresti conoscerlo come SVM o vserver. Per impostazione predefinita, Cloud Volumes ONTAP è configurato con una VM di archiviazione, ma alcune configurazioni supportano VM di archiviazione aggiuntive. È possibile specificare la VM di archiviazione per il nuovo volume.
Politica di snapshot	Una policy di copia snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot NetApp è un'immagine del file system in un dato momento che non ha alcun impatto sulle prestazioni e richiede uno spazio di archiviazione minimo. È possibile scegliere la policy predefinita o nessuna. Per i dati temporanei è possibile scegliere "nessuno": ad esempio, tempdb per Microsoft SQL Server.

b. **Protocollo**: scegliere un protocollo per il volume (NFS, CIFS o iSCSI), quindi fornire le informazioni richieste.

   Se selezioni CIFS e non è configurato alcun server, la Console ti chiederà di configurare la connettività CIFS dopo aver fatto clic su **Avanti**.

   "Scopri i protocolli e le versioni client supportati" .

   Le sezioni seguenti descrivono i campi per i quali potresti aver bisogno di assistenza. Le descrizioni sono organizzate per protocollo.

NFS

Controllo degli accessi

Scegli una policy di esportazione personalizzata per rendere il volume disponibile ai clienti.

Politica di esportazione

Definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, la Console immette un valore che fornisce l'accesso a tutte le istanze nella subnet.

CIFS

Permessi e utenti/gruppi

Consente di controllare il livello di accesso a una condivisione SMB per utenti e gruppi (chiamati anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio oppure utenti o gruppi UNIX. Se si specifica un nome utente di dominio Windows, è necessario includere il dominio dell'utente utilizzando il formato dominio\nomeutente.

Indirizzo IP primario e secondario DNS

Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS.

Se stai configurando Google Managed Active Directory, per impostazione predefinita puoi accedere ad AD con l'indirizzo IP 169.254.169.254.

Dominio Active Directory a cui unirsi

FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.

Credenziali autorizzate ad unirsi al dominio

Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.

Nome NetBIOS del server CIFS

Nome del server CIFS univoco nel dominio AD.

Unità organizzativa

L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer.

- Per configurare AWS Managed Microsoft AD come server AD per Cloud Volumes ONTAP, immettere **OU=Computers,OU=corp** in questo campo.
- Per configurare Azure AD Domain Services come server AD per Cloud Volumes ONTAP, immettere **OU=AADDC Computers** o **OU=AADDC Users** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: creare un'unità organizzativa (OU) in un dominio gestito da Azure AD Domain Services"^]
- Per configurare Google Managed Microsoft AD come server AD per Cloud Volumes ONTAP, immettere **OU=Computers,OU=Cloud** in questo campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentazione di Google Cloud: unità organizzative in Google Managed Microsoft AD"^]

Dominio DNS

Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.

Server NTP

Selezionare **Usa dominio Active Directory** per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, è necessario utilizzare l'API. Per informazioni fare riferimento al "Documentazione sull'automazione NetApp Console" .

Si noti che è possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

iSCSI

LUN

Le destinazioni di archiviazione iSCSI sono chiamate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. Quando si crea un volume iSCSI, la Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, eliminando così ogni attività di gestione. Dopo aver creato il volume,"utilizzare l'IQN per connettersi al LUN dai tuoi host" .

Gruppo iniziatore

I gruppi di iniziatori (igroup) specificano quali host possono accedere a LUN specificati sul sistema di archiviazione

Iniziatore ospite (IQN)

Le destinazioni iSCSI si connettono alla rete tramite schede di rete Ethernet standard (NIC), schede TCP offload engine (TOE) con iniziatori software, schede di rete convergenti (CNA) o adattatori host bus dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN).

a. **Tipo di disco**: scegli un tipo di disco sottostante per il volume in base alle tue esigenze di prestazioni e ai requisiti di costo.

   - "Dimensionamento del sistema in AWS"
     - "Dimensionamento del sistema in Azure"
     - "Dimensionamento del sistema in Google Cloud"

4. **Profilo di utilizzo e criteri di suddivisione in livelli**: scegli se abilitare o disabilitare le funzionalità di efficienza di archiviazione sul volume e quindi seleziona un"politica di suddivisione in livelli del volume" .

   ONTAP include diverse funzionalità di efficienza di archiviazione che possono ridurre la quantità totale di spazio di archiviazione necessario. Le funzionalità di efficienza dello storage NetApp offrono i seguenti vantaggi:

   Provisioning sottile

   Offre agli host o agli utenti più spazio di archiviazione logica di quello effettivamente disponibile nel pool di archiviazione fisico. Invece di preallocare lo spazio di archiviazione, lo spazio di archiviazione viene allocato dinamicamente a ciascun volume man mano che i dati vengono scritti.

   Deduplicazione

   Migliora l'efficienza individuando blocchi di dati identici e sostituendoli con riferimenti a un singolo blocco condiviso. Questa tecnica riduce i requisiti di capacità di archiviazione eliminando i blocchi

ridondanti di dati che risiedono nello stesso volume.

Compressione

Riduce la capacità fisica necessaria per archiviare i dati comprimendoli all'interno di un volume su storage primario, secondario e di archivio.

5. **Revisione**: rivedere i dettagli sul volume e quindi fare clic su **Aggiungi**.

Risultato

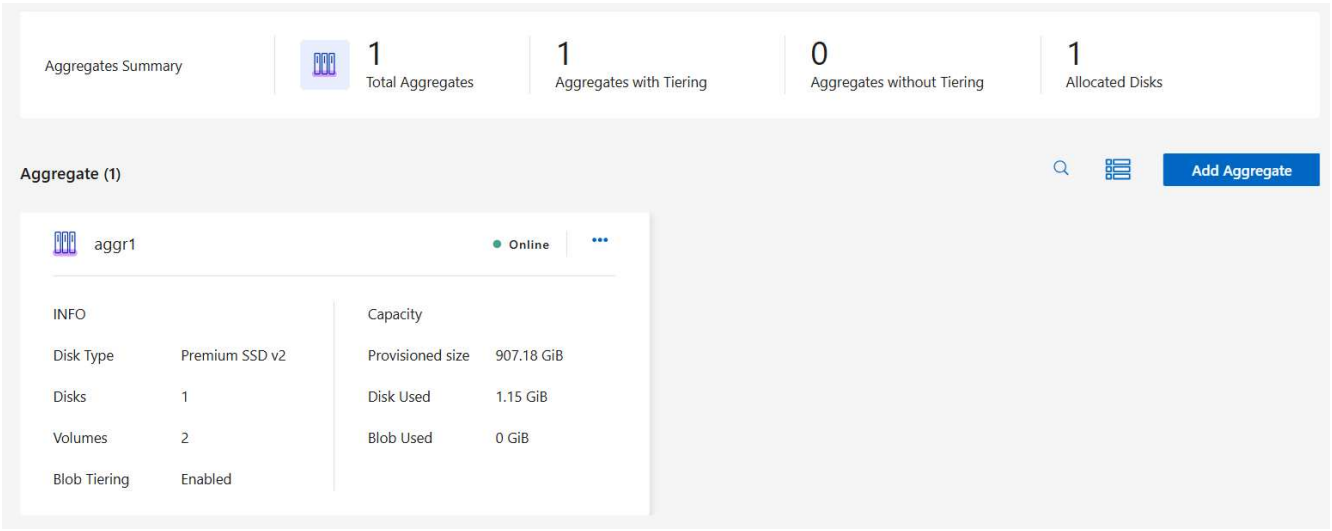
La console crea il volume sul sistema Cloud Volumes ONTAP .

Creare un volume sul secondo nodo in una configurazione HA

Per impostazione predefinita, la console crea volumi sul primo nodo in una configurazione HA. Se è necessaria una configurazione attiva-attiva, in cui entrambi i nodi forniscono dati ai client, è necessario creare aggregati e volumi sul secondo nodo.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
3. Nella scheda Aggregati, fare clic su **Aggiungi aggregato** e creare l'aggregato.



4. Per Home Node, scegliere il secondo nodo nella coppia HA.
5. Dopo che la Console ha creato l'aggregato, selezionarlo e quindi fare clic su **Crea volume**.
6. Inserisci i dettagli per il nuovo volume, quindi fai clic su **Crea**.

Risultato

La console crea il volume sul secondo nodo nella coppia HA.

Per le coppie HA distribuite in più zone di disponibilità AWS, è necessario montare il volume sui client utilizzando l'indirizzo IP mobile del nodo su cui risiede il volume.

Dopo aver creato un volume

Se hai predisposto una condivisione CIFS, assegna agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verifica che tali utenti possano accedere alla condivisione e creare un file.

Se si desidera applicare quote ai volumi, è necessario utilizzare ONTAP System Manager o ONTAP CLI. Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Gestisci i volumi sui sistemi Cloud Volumes ONTAP

È possibile gestire volumi e server CIFS nella NetApp Console. È anche possibile spostare i volumi per evitare problemi di capacità.

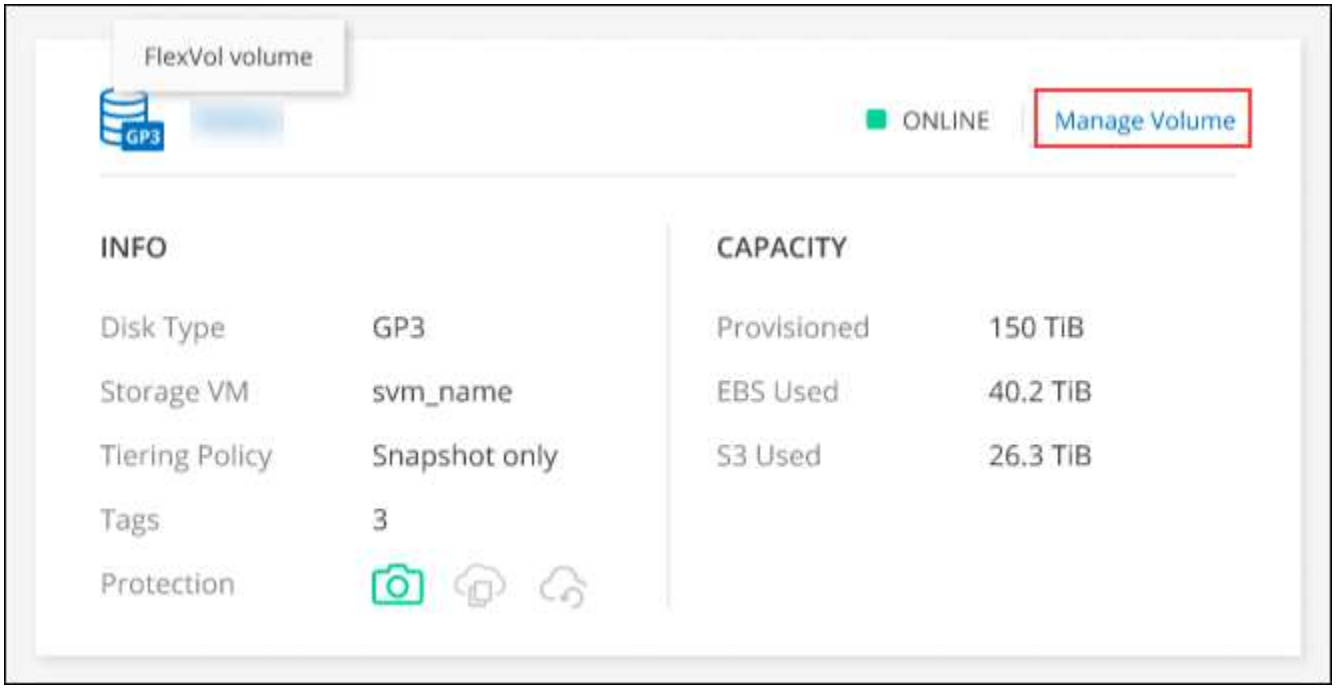
È possibile gestire i volumi nella vista standard NetApp Console oppure tramite ONTAP System Manager, incluso nella console per la gestione avanzata dei volumi. La vista standard fornisce un set limitato di opzioni per modificare i volumi. System Manager offre un livello avanzato di gestione, come la clonazione, il ridimensionamento, la modifica delle impostazioni anti-ransomware, l'analisi, la protezione e il monitoraggio delle attività, nonché lo spostamento di volumi tra livelli. Per informazioni, fare riferimento a"Amministrare Cloud Volumes ONTAP utilizzando System Manager" .

Gestire i volumi

Utilizzando la Visualizzazione standard della Console, è possibile gestire i volumi in base alle proprie esigenze di archiviazione. È possibile visualizzare, modificare, clonare, ripristinare ed eliminare i volumi.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare doppio clic sul sistema Cloud Volumes ONTAP su cui si desidera gestire i volumi.
3. Selezionare la scheda **Volumi**.



4. Nel riquadro del volume richiesto, fare clic su **Gestisci volume**.

Compito	Azione
Visualizza informazioni su un volume	In Azioni volume nel pannello Gestisci volumi, fare clic su **Visualizza dettagli volume**.
Ottieni il comando di montaggio NFS	a. In Azioni volume nel pannello Gestisci volumi, fare clic su **Comando di montaggio**. b. Fare clic su **Copia**.
Clonare un volume	a. In Azioni volume nel pannello Gestisci volumi, fare clic su **Clona il volume**. b. Modificare il nome del clone secondo necessità, quindi fare clic su **Clona**. Questo processo crea un volume FlexClone . Un volume FlexClone è una copia scrivibile, puntuale e a basso consumo di spazio, perché utilizza una piccola quantità di spazio per i metadati e consuma spazio aggiuntivo solo quando i dati vengono modificati o aggiunti. Per saperne di più sui volumi FlexClone , fare riferimento a "Guida alla gestione dell'archiviazione logica ONTAP 9" .
Modifica un volume (solo volumi di lettura-scrittura)	a. In Azioni volume nel pannello Gestisci volumi, fare clic su **Modifica impostazioni volume** b. Modificare il criterio Snapshot del volume, la versione del protocollo NFS, l'elenco di controllo degli accessi NFS (criterio di esportazione) o le autorizzazioni di condivisione, quindi fare clic su **Applica**. Se hai bisogno di policy Snapshot personalizzate, puoi crearle utilizzando ONTAP System Manager.
Elimina un volume	a. In Azioni volume nel pannello Gestisci volumi, fare clic su **Elimina il volume**. b. Nella finestra Elimina volume, immettere il nome del volume che si desidera eliminare. c. Fare nuovamente clic su **Elimina** per confermare.
Crea una copia Snapshot su richiesta	a. In Azioni di protezione nel pannello Gestisci volumi, fare clic su **Crea una copia snapshot**. b. Se necessario, modifica il nome e poi fai clic su **Crea**.
Ripristina i dati da una copia Snapshot su un nuovo volume	a. In Azioni di protezione nel pannello Gestisci volumi, fare clic su **Ripristina da copia snapshot**. b. Selezionare una copia Snapshot, immettere un nome per il nuovo volume, quindi fare clic su **Ripristina**.

Compito	Azione
Cambia il tipo di disco sottostante	a. In Azioni avanzate nel pannello Gestisci volumi, fare clic su **Cambia tipo di disco**. b. Selezionare il tipo di disco, quindi fare clic su **Cambia**. La console sposta il volume in un aggregato esistente che utilizza il tipo di disco selezionato oppure crea un nuovo aggregato per il volume.
Cambiare la politica di suddivisione in livelli	a. In Azioni avanzate nel pannello Gestisci volumi, fare clic su **Modifica criterio di suddivisione in livelli**. b. Seleziona una policy diversa e clicca su **Modifica**. La console sposta il volume in un aggregato esistente che utilizza il tipo di disco selezionato con livelli oppure crea un nuovo aggregato per il volume.
Elimina un volume	a. Selezionare un volume, quindi fare clic su **Elimina**. b. Digitare il nome del volume nella finestra di dialogo. c. Fare nuovamente clic su **Elimina** per confermare.

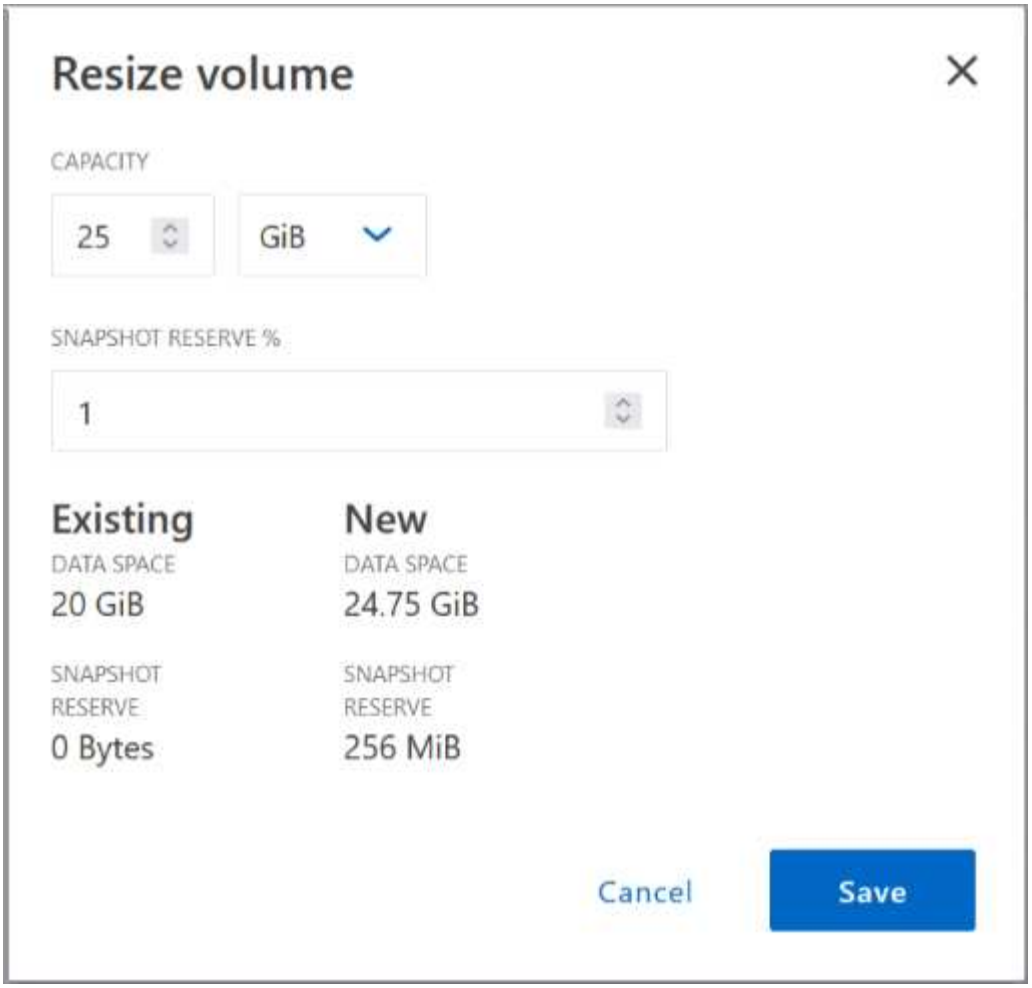
Ridimensionare un volume

Per impostazione predefinita, un volume aumenta automaticamente fino a raggiungere la dimensione massima quando lo spazio è esaurito. Il valore predefinito è 1.000, il che significa che il volume può aumentare fino a 11 volte la sua dimensione. Questo valore è configurabile nelle impostazioni dell'agente Console.

Se è necessario ridimensionare il volume, è possibile farlo da ONTAP System Manager nella Console.

Passi

1. Fare clic sulla vista System Manager per ridimensionare un volume tramite ONTAP System Manager. Fare riferimento a "Come iniziare" .
2. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Volumi**.
3. Dall'elenco dei volumi, identifica quello che vuoi ridimensionare.
4. Fare clic sull'icona delle opzioni .
5. Seleziona **Ridimensiona**.
6. Nella schermata **Ridimensiona volume**, modifica la capacità e la percentuale di riserva Snapshot come richiesto. È possibile confrontare lo spazio disponibile esistente con la capacità modificata.
7. Fare clic su **Salva**.



Quando si ridimensionano i volumi, assicurarsi di tenere in considerazione i limiti di capacità del sistema. Vai al "Note sulla versione Cloud Volumes ONTAP" per maggiori informazioni.

Modificare il server CIFS

Se si modificano i server DNS o il dominio Active Directory, è necessario modificare il server CIFS in Cloud Volumes ONTAP in modo che possa continuare a fornire spazio di archiviazione ai client.

Passi

1. Dalla scheda **Panoramica** del sistema Cloud Volumes ONTAP , fare clic sulla scheda **Funzionalità** nel pannello di destra.
2. Nel campo Configurazione CIFS, fare clic sull'icona della matita per visualizzare la finestra Configurazione CIFS.
3. Specificare le impostazioni per il server CIFS:

Compito	Azione
Seleziona VM di archiviazione (SVM)	Selezionando la macchina virtuale di archiviazione Cloud Volume ONTAP (SVM) vengono visualizzate le informazioni CIFS configurate.
Dominio Active Directory a cui unirsi	FQDN del dominio Active Directory (AD) a cui si desidera che il server CIFS si unisca.

Compito	Azione
Credenziali autorizzate ad unirsi al dominio	Nome e password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata all'interno del dominio AD.
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui verrà aggiunto il server CIFS. ifdef::gcp[] Se stai configurando Google Managed Active Directory, per impostazione predefinita è possibile accedere ad AD con l'indirizzo IP 169.254.169.254. endif::gcp[]
Dominio DNS	Dominio DNS per la macchina virtuale di archiviazione (SVM) Cloud Volumes ONTAP . Nella maggior parte dei casi, il dominio è lo stesso del dominio AD.
Nome NetBIOS del server CIFS	Nome del server CIFS univoco nel dominio AD.
Unità organizzativa	L'unità organizzativa all'interno del dominio AD da associare al server CIFS. L'impostazione predefinita è CN=Computer. • Per configurare AWS Managed Microsoft AD come server AD per Cloud Volumes ONTAP, immettere **OU=Computers,OU=corp** in questo campo. • Per configurare Azure AD Domain Services come server AD per Cloud Volumes ONTAP, immettere **OU=AADDC Computers** o **OU=AADDC Users** in questo campo."Documentazione di Azure: creare un'unità organizzativa (OU) in un dominio gestito da Azure AD Domain Services" • Per configurare Google Managed Microsoft AD come server AD per Cloud Volumes ONTAP, immettere **OU=Computers,OU=Cloud** in questo campo."Documentazione di Google Cloud: unità organizzative in Google Managed Microsoft AD"

4. Fare clic su **Imposta**.

Risultato

Cloud Volumes ONTAP aggiorna il server CIFS con le modifiche.

Spostare un volume

Spostare i volumi per sfruttare al meglio la capacità, migliorare le prestazioni e soddisfare gli accordi sul livello di servizio.

È possibile spostare un volume in ONTAP System Manager selezionando un volume e l'aggregato di destinazione, avviando l'operazione di spostamento del volume e, facoltativamente, monitorando il processo di spostamento del volume. Quando si utilizza System Manager, un'operazione di spostamento del volume viene completata automaticamente.

Passi

1. Utilizzare ONTAP System Manager o ONTAP CLI per spostare i volumi nell'aggregato.

Nella maggior parte dei casi è possibile utilizzare System Manager per spostare i volumi.

Per le istruzioni, fare riferimento al"Guida rapida per lo spostamento del volume ONTAP 9" .

Spostare un volume quando la console visualizza un messaggio di azione richiesta

La console potrebbe visualizzare un messaggio di azione richiesta che indica che è necessario spostare un volume per evitare problemi di capacità, ma che è necessario correggere il problema autonomamente. In tal caso, è necessario individuare il modo per correggere il problema e quindi spostare uno o più volumi.

La Console visualizza questi messaggi di azione richiesta quando un aggregato ha raggiunto il 90% della capacità utilizzata. Se la suddivisione in livelli dei dati è abilitata, i messaggi vengono visualizzati quando un aggregato ha raggiunto l'80% della capacità utilizzata. Per impostazione predefinita, il 10% dello spazio libero è riservato alla suddivisione in livelli dei dati. "Scopri di più sul rapporto di spazio libero per la suddivisione in livelli dei dati" .

Passi

1. Identificare come correggere i problemi di capacità .
2. In base alla tua analisi, sposta i volumi per evitare problemi di capacità:
   - Spostare i volumi su un altro sistema per evitare problemi di capacità .
   - Spostare i volumi su un altro aggregato per evitare problemi di capacità .

Identificare come correggere i problemi di capacità

Se la Console non è in grado di fornire suggerimenti per lo spostamento di un volume per evitare problemi di capacità, è necessario identificare i volumi da spostare e se spostarli su un altro aggregato sullo stesso sistema o su un altro sistema.

Passi

1. Visualizzare le informazioni avanzate nel messaggio Azione richiesta per identificare l'aggregato che ha raggiunto il limite di capacità.

   Ad esempio, le informazioni avanzate dovrebbero contenere un messaggio simile a quanto segue: Aggregate aggr1 ha raggiunto il limite di capacità.

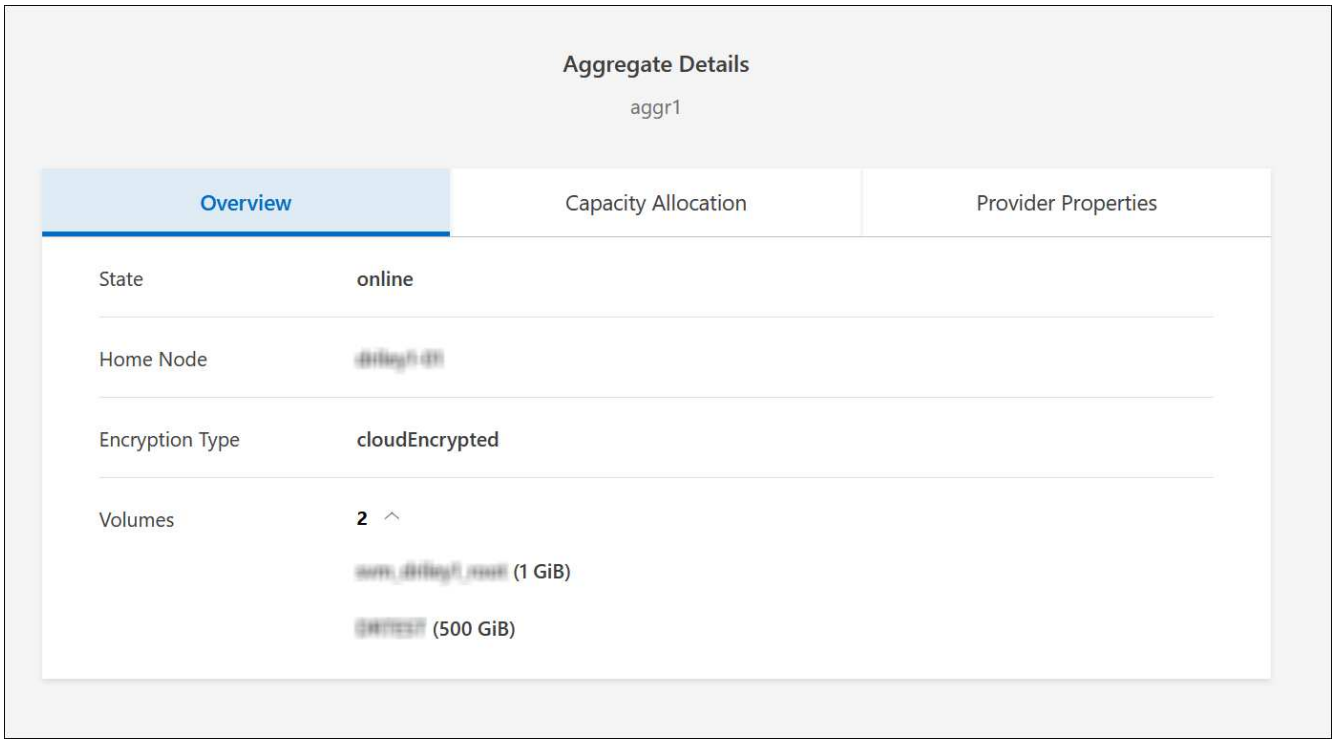
2. Identificare uno o più volumi da spostare fuori dall'aggregato:

   a. Nel sistema Cloud Volumes ONTAP , fare clic sulla scheda **Aggregati**.

   b. Nel riquadro aggregato, fare clic su ••• icona e quindi fare clic su **Visualizza dettagli aggregati**.

   c. Nella scheda **Panoramica** della schermata **Dettagli aggregati**, controlla le dimensioni di ciascun volume e scegli uno o più volumi da spostare fuori dall'aggregato.

      Dovresti scegliere volumi sufficientemente grandi da liberare spazio complessivamente, in modo da evitare ulteriori problemi di capacità in futuro.



3. Se il sistema non ha raggiunto il limite del disco, è necessario spostare i volumi su un aggregato esistente o su un nuovo aggregato sullo stesso sistema.

   Per informazioni, fare riferimento aSpostare i volumi su un altro aggregato per evitare problemi di capacità .

4. Se il sistema ha raggiunto il limite del disco, procedere come segue:
   a. Eliminare tutti i volumi non utilizzati.
   b. Riorganizzare i volumi per liberare spazio su un aggregato.

      Per informazioni, fare riferimento aSpostare i volumi su un altro aggregato per evitare problemi di capacità .

   c. Spostare due o più volumi su un altro sistema che abbia spazio.

      Per informazioni, fare riferimento aSpostare i volumi su un altro aggregato per evitare problemi di capacità .

Spostare i volumi su un altro sistema per evitare problemi di capacità

È possibile spostare uno o più volumi su un altro sistema Cloud Volumes ONTAP per evitare problemi di capacità. Potrebbe essere necessario eseguire questa operazione se il sistema ha raggiunto il limite del disco.

Informazioni su questo compito

È possibile seguire i passaggi descritti in questa attività per correggere il seguente messaggio di azione richiesta:

> Lo spostamento di un volume è necessario per evitare problemi di capacità; tuttavia, la Console non può eseguire questa azione perché il sistema ha raggiunto il limite del disco.

Passi

1. Identificare un sistema Cloud Volumes ONTAP con capacità disponibile oppure distribuire un nuovo sistema.
2. Trascinare e rilasciare il sistema di origine sul sistema di destinazione per eseguire una replica dei dati una tantum del volume.

   Per informazioni, fare riferimento a"Replica dei dati tra i sistemi" .
3. Accedere alla pagina Stato replicazione, quindi interrompere la relazione SnapMirror per convertire il volume replicato da un volume di protezione dati a un volume di lettura/scrittura.

   Per informazioni, fare riferimento a"Gestione delle pianificazioni e delle relazioni di replicazione dei dati" .
4. Configurare il volume per l'accesso ai dati.

   Per informazioni sulla configurazione di un volume di destinazione per l'accesso ai dati, fare riferimento a"Guida rapida al ripristino di emergenza del volume ONTAP 9" .
5. Elimina il volume originale.

   Per informazioni, fare riferimento a"Gestire i volumi" .

Spostare i volumi su un altro aggregato per evitare problemi di capacità

È possibile spostare uno o più volumi su un altro aggregato per evitare problemi di capacità.

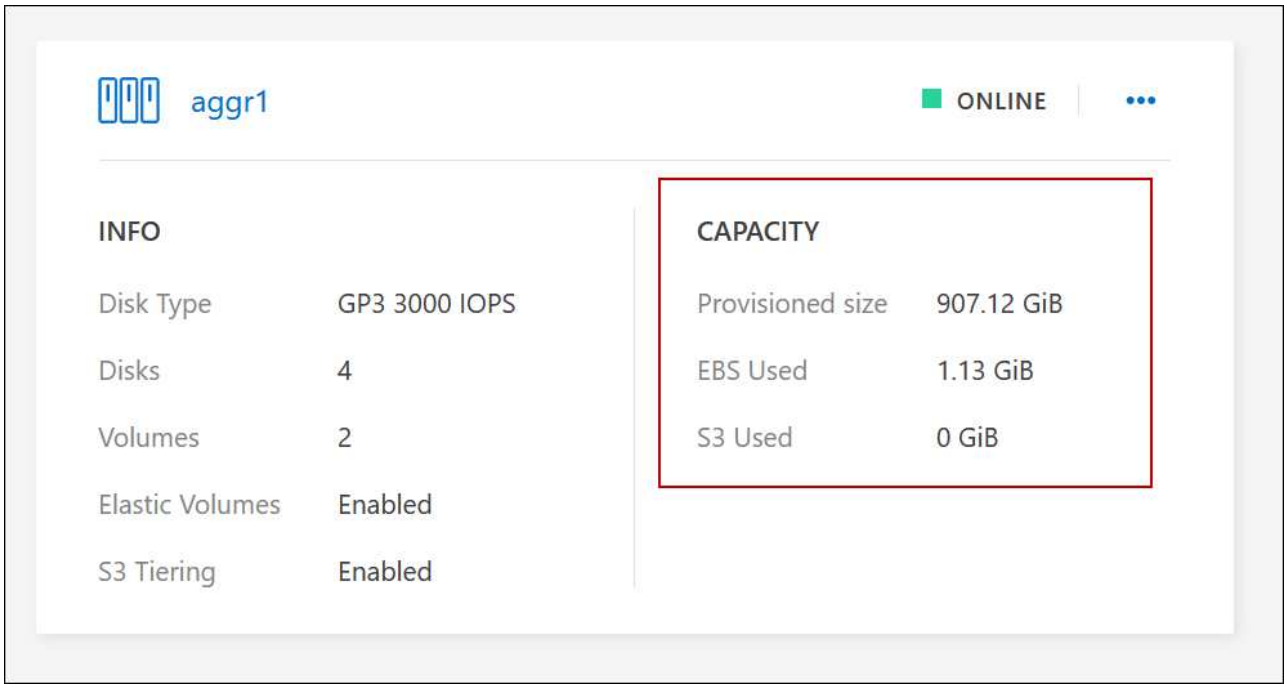
Informazioni su questo compito

È possibile seguire i passaggi descritti in questa attività per correggere il seguente messaggio di azione richiesta:

> Per evitare problemi di capacità è necessario spostare due o più volumi; tuttavia, la Console non può eseguire questa azione per te.

Passi

1. Verificare se un aggregato esistente ha capacità disponibile per i volumi che è necessario spostare:
   a. Nel sistema Cloud Volumes ONTAP , fare clic sulla scheda **Aggregati**.
   b. Sulla tessera aggregata richiesta, fare clic su ••• icona e quindi **Visualizza dettagli aggregati** per visualizzare la capacità disponibile (dimensione fornita meno capacità aggregata utilizzata).



2. Se necessario, aggiungere dischi a un aggregato esistente:
   a. Selezionare l'aggregato, quindi fare clic su ••• icona > **Aggiungi dischi**.
   b. Selezionare il numero di dischi da aggiungere, quindi fare clic su **Aggiungi**.
3. Se nessun aggregato ha capacità disponibile, crea un nuovo aggregato.

   Per informazioni, fare riferimento a"Creazione di aggregati" .
4. Utilizzare ONTAP System Manager o ONTAP CLI per spostare i volumi nell'aggregato.
5. Nella maggior parte dei casi è possibile utilizzare System Manager per spostare i volumi.

   Per le istruzioni, fare riferimento al"Guida rapida per lo spostamento del volume ONTAP 9" .

Motivi per cui un movimento di volume potrebbe essere lento

Lo spostamento di un volume potrebbe richiedere più tempo del previsto se una delle seguenti condizioni è vera per Cloud Volumes ONTAP:

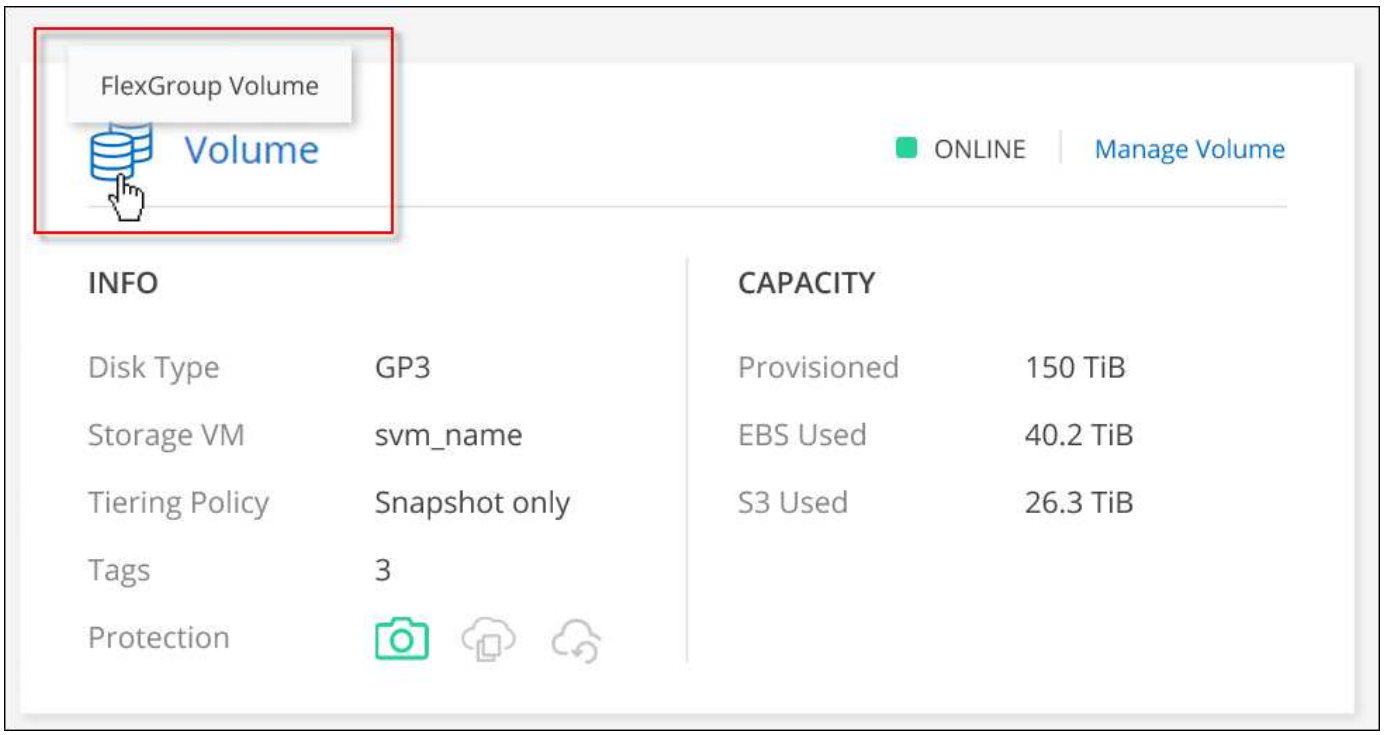
- Il volume è un clone.
- Il volume è il genitore di un clone.
- L'aggregato di origine o di destinazione ha un singolo disco Throughput Optimized HDD (st1).
- Uno degli aggregati utilizza uno schema di denominazione più vecchio per gli oggetti. Entrambi gli aggregati devono utilizzare lo stesso formato di nome.

  Se la suddivisione in livelli dei dati è stata abilitata su un aggregato nella versione 9.4 o in una versione precedente, viene utilizzato uno schema di denominazione precedente.
- Le impostazioni di crittografia non corrispondono negli aggregati di origine e di destinazione oppure è in corso una nuova chiave.
- L'opzione *-tiering-policy* è stata specificata durante lo spostamento del volume per modificare la politica di suddivisione in livelli.

- L'opzione *-generate-destination-key* è stata specificata durante lo spostamento del volume.

Visualizza i volumi FlexGroup

È possibile visualizzare i volumi FlexGroup creati tramite ONTAP System Manager o ONTAP CLI direttamente tramite la scheda Volumi nella Console. È possibile visualizzare informazioni dettagliate sui volumi FleGroup tramite un riquadro dedicato **Volumi**, in cui è possibile identificare ciascun gruppo di volumi FlexGroup tramite il testo passante sull'icona. Inoltre, è possibile identificare e ordinare i volumi FlexGroup nella vista elenco volumi tramite la colonna Stile volume.



Attualmente, nella Console è possibile visualizzare solo i volumi FlexGroup esistenti. Non è possibile creare volumi FlexGroup nella Console.

Trasferisci i dati Cloud Volumes ONTAP inattivi in un archivio di oggetti a basso costo

È possibile ridurre i costi di archiviazione per Cloud Volumes ONTAP combinando un livello di prestazioni SSD o HDD per i dati attivi con un livello di capacità di archiviazione degli oggetti per i dati inattivi. La suddivisione in livelli dei dati è basata sulla tecnologia FabricPool . Per una panoramica di alto livello, fare riferimento a"Panoramica della suddivisione in livelli dei dati" .

Per impostare la suddivisione in livelli dei dati, è necessario procedere come segue:

1 Scegli una configurazione supportata

Sono supportate la maggior parte delle configurazioni. Se disponi di un sistema Cloud Volumes ONTAP che esegue la versione più recente, sei a posto. "Saperne di più" .

2 Garantire la connettività tra Cloud Volumes ONTAP e l'archiviazione degli oggetti

- Per AWS, avrai bisogno di un endpoint VPC per Amazon Simple Storage Service (Amazon S3). Saperne di più.
- Per Azure, non sarà necessario fare nulla finché la NetApp Console avrà le autorizzazioni necessarie. Saperne di più .
- Per Google Cloud, è necessario configurare la subnet per l'accesso privato a Google e impostare un account di servizio. Saperne di più .

3 Assicurati di avere un aggregato con livelli abilitati

Per abilitare la suddivisione in livelli dei dati su un aggregato, è necessario abilitarla su un volume. È necessario conoscere i requisiti per i nuovi volumi e per quelli esistenti. Saperne di più .

4 Scegliere una politica di suddivisione in livelli durante la creazione, la modifica o la replica di un volume

La NetApp Console richiede di scegliere una policy di suddivisione in livelli quando si crea, si modifica o si replica un volume.

- "Suddivisione dei dati dai volumi di lettura-scrittura"
- "Livelli di dati dai volumi di protezione dei dati"

Cosa non è necessario per la suddivisione in livelli dei dati?

- Per abilitare la suddivisione in livelli dei dati non è necessario installare una licenza per le funzionalità.
- Non è necessario creare un archivio oggetti per il livello di capacità. La Console lo fa per te.
- Non è necessario abilitare la suddivisione in livelli dei dati a livello di sistema.

  La console crea un archivio oggetti per i dati freddi quando crea il sistema,finché non ci sono problemi di connettività o di permessi . Dopodiché, è sufficiente abilitare la suddivisione in livelli dei dati sui volumi (e in alcuni casi,sugli aggregati).

Configurazioni che supportano la suddivisione in livelli dei dati

È possibile abilitare la suddivisione in livelli dei dati quando si utilizzano configurazioni e funzionalità specifiche.

Supporto in AWS

- La suddivisione in livelli dei dati è supportata in AWS a partire da Cloud Volumes ONTAP 9.2.
- Il livello di prestazioni può essere costituito da SSD per uso generico (gp3 o gp2) o SSD Provisioned IOPS (io1).

Si sconsiglia di suddividere i dati in livelli per l'archiviazione di oggetti quando si utilizzano HDD Throughput Optimized (st1).

- I dati inattivi vengono suddivisi in livelli nei bucket Amazon S3. Il passaggio ad altri provider non è supportato.

Supporto in Azure

- In Azure è supportata la suddivisione in livelli dei dati come segue:
  - Versione 9.4 in con sistemi a nodo singolo
  - Versione 9.6 con coppie HA
- Il livello di prestazioni può essere costituito da dischi gestiti Premium SSD, dischi gestiti Standard SSD o dischi gestiti Standard HDD.
- I dati inattivi sono suddivisi in livelli in Microsoft Azure Blob. Il passaggio ad altri provider non è supportato.

Supporto in Google Cloud

- La suddivisione in livelli dei dati è supportata in Google Cloud a partire da Cloud Volumes ONTAP 9.6.
- Il livello di prestazioni può essere costituito da dischi persistenti SSD, dischi persistenti bilanciati o dischi persistenti standard.
- I dati inattivi vengono archiviati su Google Cloud Storage. Il passaggio ad altri provider non è supportato.

Interoperabilità delle funzionalità

- La suddivisione in livelli dei dati è supportata da tecnologie di crittografia.
- Il thin provisioning deve essere abilitato sui volumi.

Requisiti

A seconda del provider cloud, è necessario impostare determinate connessioni e autorizzazioni affinché Cloud Volumes ONTAP possa suddividere i dati inattivi nell'archiviazione degli oggetti.

Requisiti per il tiering dei dati cold su Amazon S3

Assicurarsi che Cloud Volumes ONTAP abbia una connessione ad Amazon S3. Il modo migliore per fornire tale connessione è creare un endpoint VPC per il servizio S3. Per istruzioni, fare riferimento a "Documentazione AWS: creazione di un endpoint gateway".

Quando crei l'endpoint VPC, assicurati di selezionare la regione, la VPC e la tabella di routing che corrispondono all'istanza Cloud Volumes ONTAP . È inoltre necessario modificare il gruppo di sicurezza per aggiungere una regola HTTPS in uscita che consenta il traffico verso l'endpoint S3. In caso contrario, Cloud Volumes ONTAP non potrà connettersi al servizio S3.

Se riscontri problemi, fai riferimento a "AWS Support Knowledge Center: perché non riesco a connettermi a un bucket S3 tramite un endpoint VPC gateway?" .

Requisiti per suddividere i dati inattivi in livelli nell'archiviazione BLOB di Azure

Non è necessario impostare una connessione tra il livello di prestazioni e il livello di capacità, purché la Console disponga delle autorizzazioni richieste. La Console abilita un endpoint del servizio VNet se il ruolo personalizzato per l'agente della Console dispone delle seguenti autorizzazioni:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Il ruolo personalizzato include le autorizzazioni per impostazione predefinita. "Visualizza l'autorizzazione di Azure per l'agente della console"

Requisiti per suddividere i dati inattivi in un bucket di Google Cloud Storage

- La subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per le istruzioni, fare riferimento a "Documentazione di Google Cloud: configurazione dell'accesso privato a Google" .
- È necessario collegare un account di servizio a Cloud Volumes ONTAP.

  "Scopri come configurare questo account di servizio" .

  Quando si crea un sistema Cloud Volumes ONTAP , viene richiesto di selezionare questo account di servizio.

  Se non selezioni un account di servizio durante la distribuzione, dovrai arrestare Cloud Volumes ONTAP, accedere a Google Cloud Console e quindi collegare l'account di servizio alle istanze di Cloud Volumes ONTAP. Puoi quindi abilitare il tiering dei dati come descritto nella sezione successiva.

- Per crittografare il bucket con chiavi di crittografia gestite dal cliente, abilitare il bucket di archiviazione Google Cloud in modo che utilizzi la chiave.

  "Scopri come utilizzare le chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP" .

Abilitare la suddivisione in livelli dei dati dopo aver implementato i requisiti

La console crea un archivio oggetti per i dati inattivi quando viene creato il sistema, a condizione che non vi siano problemi di connettività o di autorizzazioni. Se non hai implementato i requisiti elencati sopra prima di aver creato il sistema, dovrai abilitare manualmente la suddivisione in livelli tramite l'API o ONTAP System Manager, che crea l'archivio oggetti.

ⓘ La possibilità di abilitare la suddivisione in livelli tramite la Console sarà disponibile in una futura versione Cloud Volumes ONTAP .

Assicurarsi che la suddivisione in livelli sia abilitata sugli aggregati

Per abilitare la suddivisione in livelli dei dati su un volume, è necessario abilitare la suddivisione in livelli dei dati su un aggregato. È necessario conoscere i requisiti per i nuovi volumi e per quelli esistenti.

- **Nuovi volumi**

  Se si abilita la suddivisione in livelli dei dati su un nuovo volume, non è necessario preoccuparsi di abilitare la suddivisione in livelli dei dati su un aggregato. La console crea il volume su un aggregato esistente con la suddivisione in livelli abilitata oppure crea un nuovo aggregato per il volume se non esiste già un aggregato con la suddivisione in livelli dei dati abilitata.

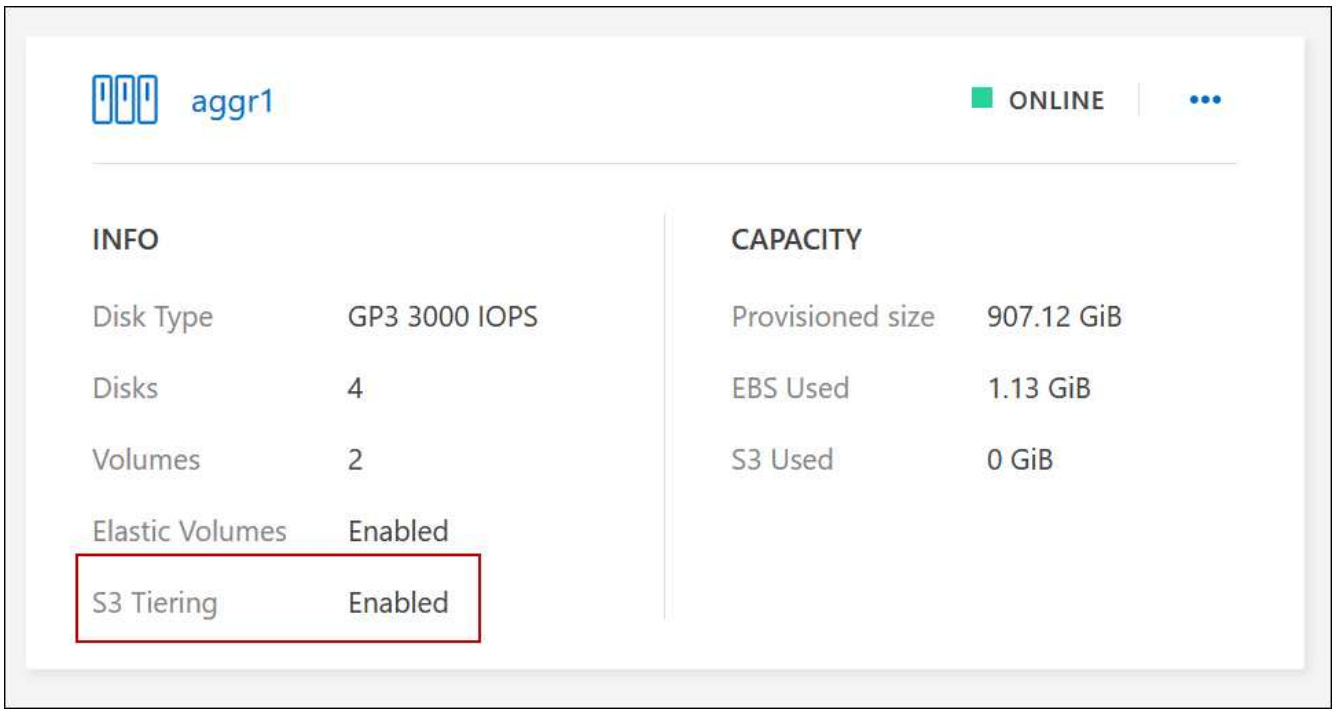
- **Volumi esistenti**

  Per abilitare la suddivisione in livelli dei dati su un volume esistente, assicurarsi che sia abilitata

sull'aggregato sottostante. Se la suddivisione in livelli dei dati non è abilitata sull'aggregato esistente, sarà necessario utilizzare ONTAP System Manager per collegare un aggregato esistente all'archivio oggetti.

Passaggi per confermare se la suddivisione in livelli è abilitata su un aggregato

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Aprire il sistema Cloud Volumes ONTAP .
3. Selezionare la scheda **Aggregati** e verificare se la suddivisione in livelli è abilitata o disabilitata sull'aggregato.



Passaggi per abilitare la suddivisione in livelli su un aggregato

1. In ONTAP System Manager, fare clic su **Archiviazione > Livelli**.
2. Fare clic sul menu delle azioni per l'aggregato e selezionare **Collega livelli cloud**.
3. Seleziona il livello cloud da collegare e fai clic su **Salva**.

Cosa succederà ora?

Ora è possibile abilitare la suddivisione in livelli dei dati su volumi nuovi ed esistenti, come spiegato nella sezione successiva.

Suddivisione dei dati dai volumi di lettura-scrittura

Cloud Volumes ONTAP può suddividere i dati inattivi sui volumi di lettura-scrittura in un archivio di oggetti conveniente, liberando il livello delle prestazioni per i dati attivi.

Passi

1. Nella scheda **Volumi** del sistema, crea un nuovo volume o modifica il livello di un volume esistente:

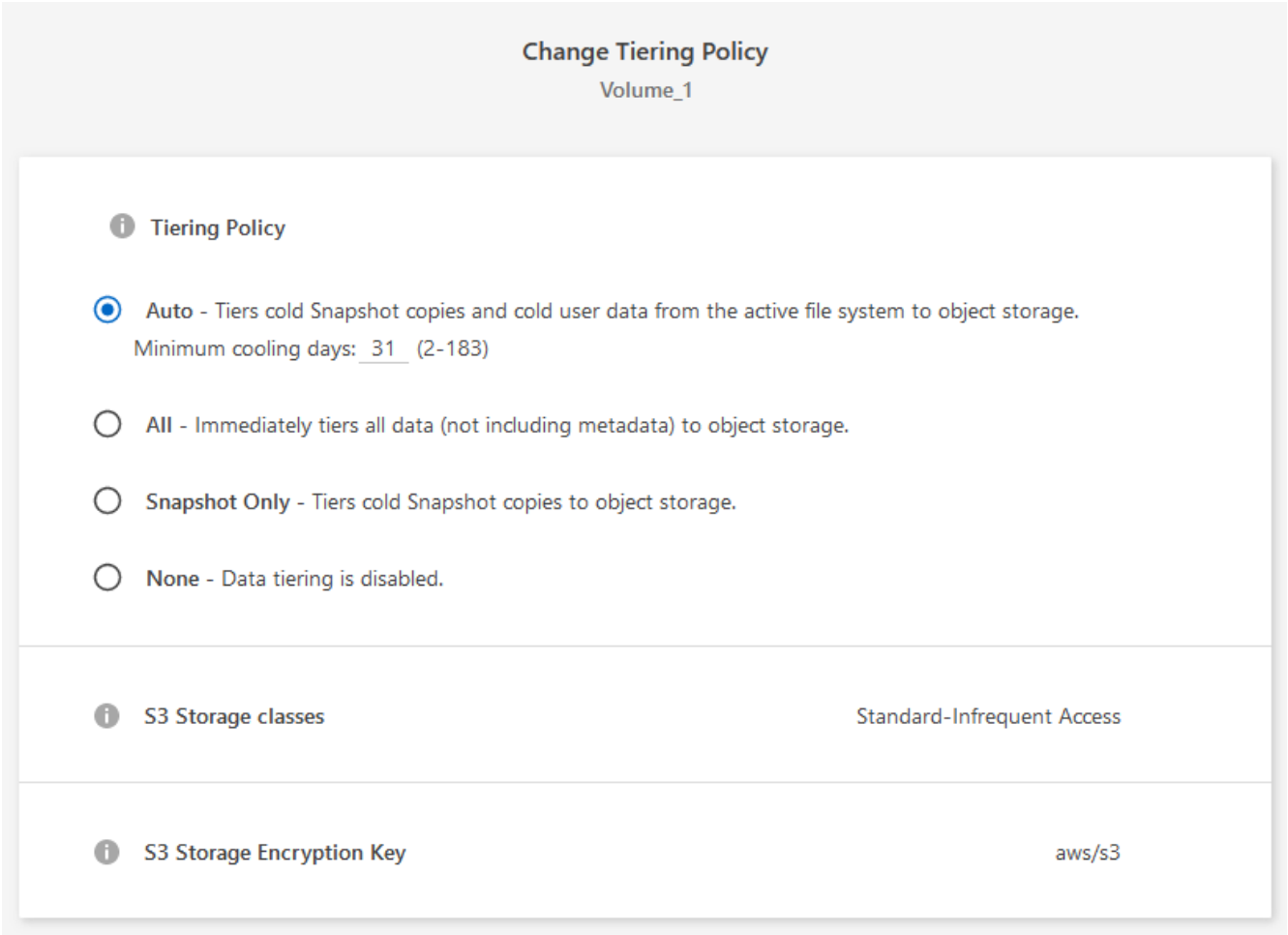
Compito	Azione
Crea un nuovo volume	Fare clic su **Aggiungi nuovo volume**.

Compito	Azione
Modificare un volume esistente	Selezionare il riquadro del volume desiderato, fare clic su **Gestisci volume** per accedere al pannello destro Gestisci volumi, quindi fare clic su **Azioni avanzate** e **Modifica criterio di suddivisione in livelli** nel pannello destro.

2. Selezionare una politica di suddivisione in livelli.

   Per una descrizione di queste politiche, fare riferimento a"Panoramica della suddivisione in livelli dei dati" .

   Esempio



   La console crea un nuovo aggregato per il volume se non esiste già un aggregato abilitato per il tiering dei dati.

Livelli di dati dai volumi di protezione dei dati

Cloud Volumes ONTAP può suddividere i dati da un volume di protezione dati a un livello di capacità. Se si attiva il volume di destinazione, i dati vengono gradualmente spostati al livello di prestazioni durante la lettura.

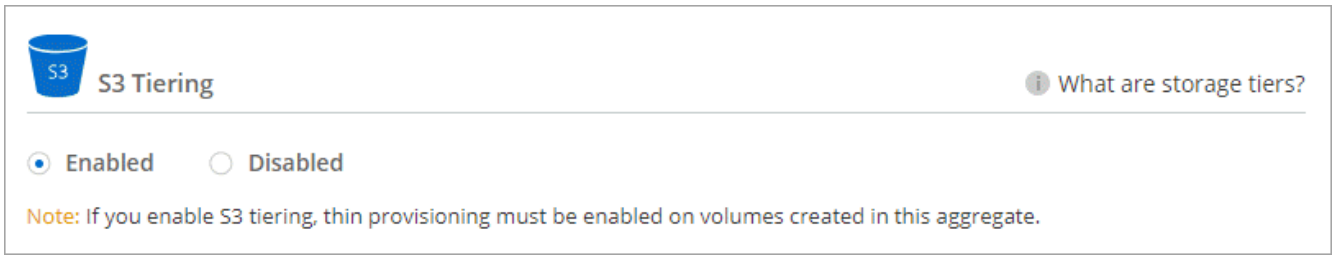
Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, seleziona il sistema Cloud Volumes ONTAP che contiene il volume di origine, quindi

trascinalo sul sistema su cui desideri replicare il volume.

3. Seguire le istruzioni fino a raggiungere la pagina di suddivisione in livelli e abilitare la suddivisione dei dati in livelli per l'archiviazione degli oggetti.

Esempio



Per assistenza con la replica dei dati, fare riferimento a "Replica dei dati da e verso il cloud" .

Modificare la classe di archiviazione per i dati a livelli

Dopo aver distribuito Cloud Volumes ONTAP, puoi ridurre i costi di archiviazione modificando la classe di archiviazione per i dati inattivi a cui non si è avuto accesso per 30 giorni. I costi di accesso sono più elevati se si accede ai dati, quindi è necessario tenerne conto prima di modificare la classe di archiviazione.

La classe di archiviazione per i dati a livelli è a livello di sistema, non per volume.

Per informazioni sulle classi di archiviazione supportate, fare riferimento a"Panoramica della suddivisione in livelli dei dati" .

Passi

1. Nel sistema Cloud Volumes ONTAP , fare clic sull'icona del menu e quindi su **Classi di archiviazione** o **Suddivisione in livelli di archiviazione BLOB**.
2. Selezionare una classe di archiviazione e quindi fare clic su **Salva**.

Modifica il rapporto di spazio libero per la suddivisione in livelli dei dati

Il rapporto di spazio libero per il tiering dei dati definisce la quantità di spazio libero richiesta sugli SSD/HDD Cloud Volumes ONTAP quando si suddividono i dati in livelli per l'archiviazione degli oggetti. L'impostazione predefinita è il 10% di spazio libero, ma è possibile modificarla in base alle proprie esigenze.

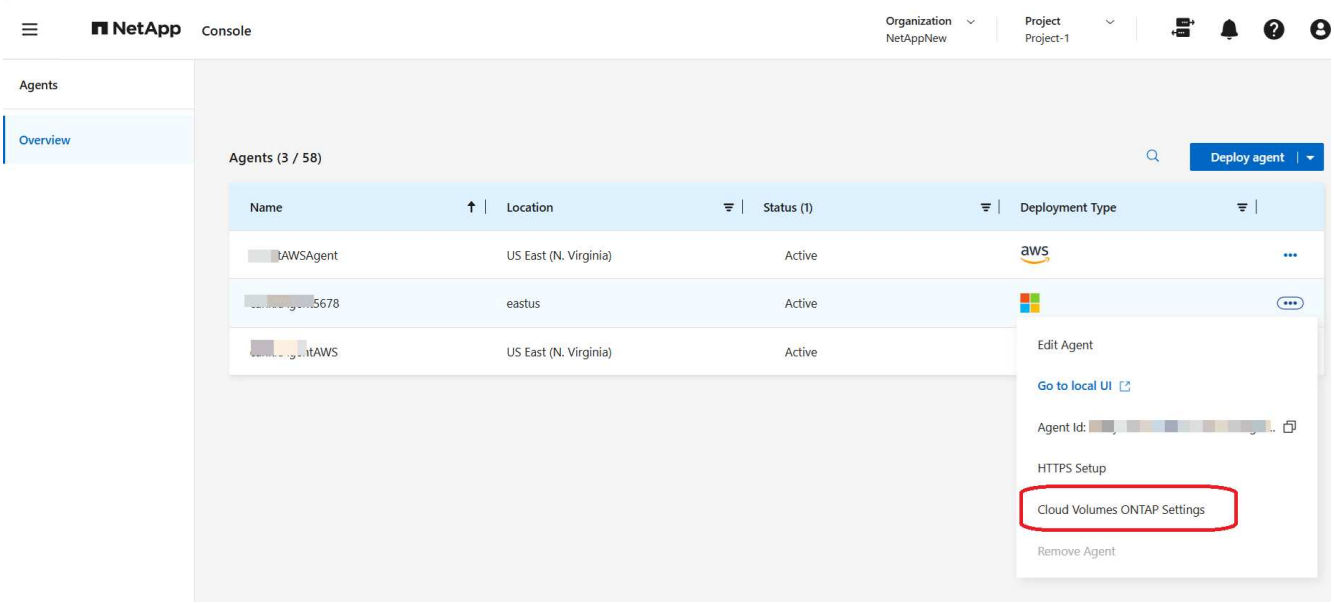
Ad esempio, potresti scegliere meno del 10% di spazio libero per assicurarti di utilizzare la capacità acquistata. La Console può quindi acquistare dischi aggiuntivi per te quando è necessaria ulteriore capacità (fino al raggiungimento del limite di dischi per l'aggregato).

Se lo spazio non è sufficiente, Cloud Volumes ONTAP non riesce a spostare i dati e si potrebbe verificare un calo delle prestazioni. Ogni modifica deve essere effettuata con cautela. In caso di dubbi, contattare l'assistenza NetApp per ricevere assistenza.

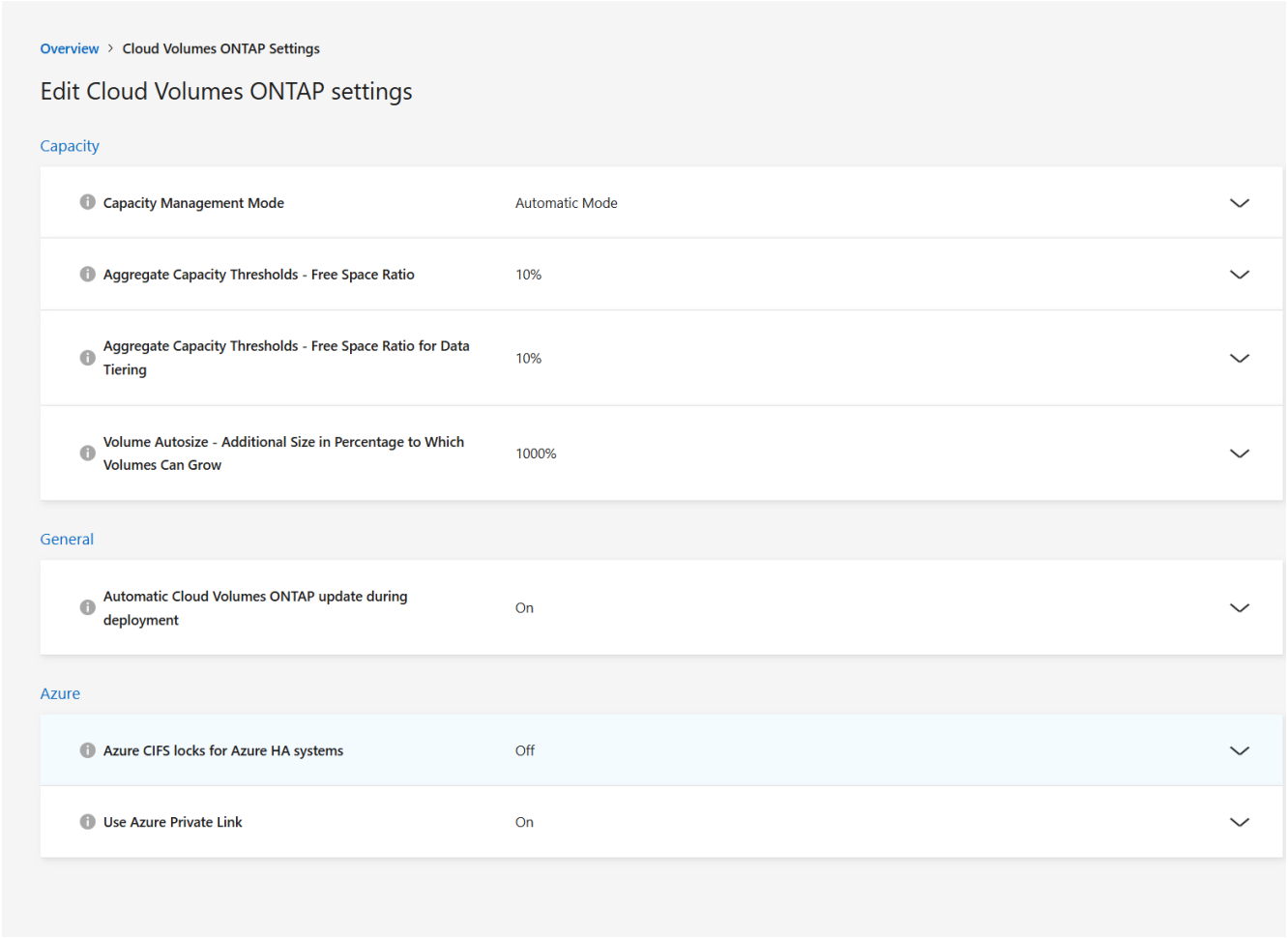
Il rapporto è importante per gli scenari di disaster recovery perché quando i dati vengono letti dall'archivio oggetti, Cloud Volumes ONTAP sposta i dati su SSD/HDD per garantire prestazioni migliori. Se lo spazio non è sufficiente, Cloud Volumes ONTAP non può spostare i dati. Tieni presente questo aspetto quando modifichi il rapporto, in modo da soddisfare le tue esigenze aziendali.

Passi

1. Dal riquadro di navigazione a sinistra, vai su **Amministrazione > Agenti**.
2. Fare clic su ••• icona per l'agente Console che gestisce il sistema Cloud Volumes ONTAP .
3. Selezionare *Impostazioni Cloud Volumes ONTAP *.



4. In **Capacità**, fare clic su **Soglie di capacità aggregata - Rapporto spazio libero per la suddivisione in livelli dei dati**.



5. Modifica la percentuale di spazio libero in base alle tue esigenze e fai clic su **Salva**.

Modificare il periodo di raffreddamento per la politica di suddivisione automatica in livelli

Se hai abilitato il tiering dei dati su un volume Cloud Volumes ONTAP utilizzando il criterio di tiering *auto*, puoi adattare il periodo di raffreddamento predefinito in base alle tue esigenze aziendali. Questa azione è supportata solo tramite ONTAP CLI e API.

Il periodo di raffreddamento è il numero di giorni per cui i dati utente in un volume devono rimanere inattivi prima che vengano considerati "freddi" e spostati nell'archiviazione degli oggetti.

Il periodo di raffreddamento predefinito per la politica di suddivisione automatica in livelli è di 31 giorni. È possibile modificare il periodo di raffreddamento come segue:

- 9.8 o successivo: da 2 giorni a 183 giorni
- 9.7 o precedente: da 2 a 63 giorni

Fare un passo

1. Utilizzare il parametro *minimumCoolingDays* con la richiesta API quando si crea un volume o si modifica un volume esistente.

Rimuovere un bucket S3 durante la dismissione di un sistema

È possibile eliminare un bucket S3 con i dati suddivisi in livelli da un sistema Cloud Volumes ONTAP quando si dismette l'ambiente.

È possibile eliminare il bucket S3 solo se:

- Il sistema Cloud Volume ONTAP viene eliminato dalla Console.
- Tutti gli oggetti vengono eliminati dal bucket e il bucket S3 è vuoto.

Quando si dismette un sistema Cloud Volumes ONTAP , il bucket S3 creato per l'ambiente non viene eliminato automaticamente. Invece, rimane in uno stato orfano per impedire qualsiasi perdita accidentale di dati. È possibile eliminare gli oggetti nel bucket, quindi rimuovere il bucket S3 stesso oppure conservarlo per un uso successivo. Fare riferimento a "ONTAP CLI: eliminazione bucket server-archivio-oggetto vserver" .

Connettiti a un LUN su Cloud Volumes ONTAP dal tuo sistema host

Quando si crea un volume iSCSI, la NetApp Console crea automaticamente un LUN. Abbiamo semplificato il tutto creando una sola LUN per volume, eliminando così ogni attività di gestione. Dopo aver creato il volume, utilizzare l'IQN per connettersi alla LUN dagli host.

Notare quanto segue:

- La gestione automatica della capacità della Console non si applica alle LUN. Quando crea un LUN, disabilita la funzionalità di aumento automatico.
- È possibile creare LUN aggiuntivi da ONTAP System Manager o da ONTAP CLI.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.

2. Nella pagina **Sistemi**, fare doppio clic sul sistema Cloud Volumes ONTAP su cui si desidera gestire i volumi.
3. Nel sistema, selezionare la scheda **Volumi**.
4. Vai al riquadro del volume richiesto e seleziona **Gestisci volume** per accedere al pannello Gestisci volumi sulla destra.
5. Fare clic su **Target iQN**.
6. Fare clic su **Copia** per copiare il nome iQN.
7. Impostare una connessione iSCSI dall'host al LUN.
    - "Configurazione ONTAP 9 iSCSI express per Red Hat Enterprise Linux: avvio delle sessioni iSCSI con la destinazione"
    - "Configurazione ONTAP 9 iSCSI express per Windows: avvio di sessioni iSCSI con la destinazione"
    - "Configurazione host SAN ONTAP"

Accelera l'accesso ai dati con i volumi FlexCache su un sistema Cloud Volumes ONTAP

Un volume FlexCache è un volume di archiviazione che memorizza nella cache i dati di lettura SMB e NFS da un volume di origine (o sorgente). Le letture successive dei dati memorizzati nella cache consentono un accesso più rapido a tali dati.

È possibile utilizzare i volumi FlexCache per velocizzare l'accesso ai dati o per scaricare il traffico dai volumi a cui si accede più frequentemente. I volumi FlexCache contribuiscono a migliorare le prestazioni, soprattutto quando i client devono accedere ripetutamente agli stessi dati, perché i dati possono essere forniti direttamente senza dover accedere al volume di origine. I volumi FlexCache sono adatti per carichi di lavoro di sistema che richiedono molta lettura.

NetApp Console fornisce la gestione dei volumi FlexCache con"NetApp Volume Caching" .

È anche possibile utilizzare ONTAP CLI o ONTAP System Manager per creare e gestire i volumi FlexCache :

- "Guida introduttiva ai volumi FlexCache per un accesso più rapido ai dati"
- "Creazione di volumi FlexCache in System Manager"

Lavora con FlexCache quando l'origine è crittografata

Quando si configura FlexCache su un sistema Cloud Volumes ONTAP in cui il volume di origine è crittografato, sono necessari passaggi aggiuntivi per garantire che il volume FlexCache possa accedere correttamente ai dati crittografati e memorizzarli nella cache.

Prima di iniziare

1. **Configurazione della crittografia**: assicurarsi che il volume di origine sia completamente crittografato e operativo. Per i sistemi Cloud Volumes ONTAP , ciò comporta l'integrazione con servizi di gestione delle chiavi specifici del cloud.

Per AWS, questo in genere significa utilizzare AWS Key Management Service (KMS). Per informazioni, fare riferimento a"Gestisci le chiavi con AWS Key Management Service" .

Per Azure, è necessario configurare Azure Key Vault per NetApp Volume Encryption (NVE). Per informazioni, fare riferimento a"Gestisci le chiavi con Azure Key Vault" .

Per Google Cloud, si tratta di Google Cloud Key Management Service. Per informazioni, fare riferimento a"Gestisci le chiavi con il servizio Cloud Key Management di Google" .

1. **Servizi di gestione delle chiavi**: prima di creare un volume FlexCache , verificare che i servizi di gestione delle chiavi siano configurati correttamente sul sistema Cloud Volumes ONTAP . Questa configurazione è essenziale affinché il volume FlexCache decrittografi i dati dal volume di origine.
2. **Licenza**: verificare che una licenza FlexCache valida sia disponibile e attivata sul sistema Cloud Volumes ONTAP .
3. * Versione ONTAP *: assicurati che la versione ONTAP del tuo sistema Cloud Volumes ONTAP supporti FlexCache con volumi crittografati. Fare riferimento alle ultime "Note sulla versione ONTAP" o matrice di compatibilità per maggiori informazioni.
4. **Configurazione di rete**: assicurarsi che la configurazione di rete consenta una comunicazione fluida tra il volume di origine e il volume FlexCache . Ciò include il routing corretto e la risoluzione DNS in un ambiente

cloud.

Passi

Crea un volume FlexCache sul tuo sistema Cloud Volumes ONTAP con un volume sorgente crittografato. Per passaggi dettagliati e considerazioni aggiuntive, fare riferimento alle seguenti sezioni:

- "Guida introduttiva ai volumi FlexCache per un accesso più rapido ai dati"
- "Creazione di volumi FlexCache in System Manager"

Amministrazione aggregata

Creare un aggregato per i sistemi Cloud Volumes ONTAP

Puoi creare gli aggregati autonomamente oppure lasciare che sia la NetApp Console a farlo per te quando crea i volumi. Il vantaggio di creare autonomamente gli aggregati è che puoi scegliere la dimensione del disco sottostante, il che ti consente di dimensionare l'aggregato in base alla capacità o alle prestazioni di cui hai bisogno.

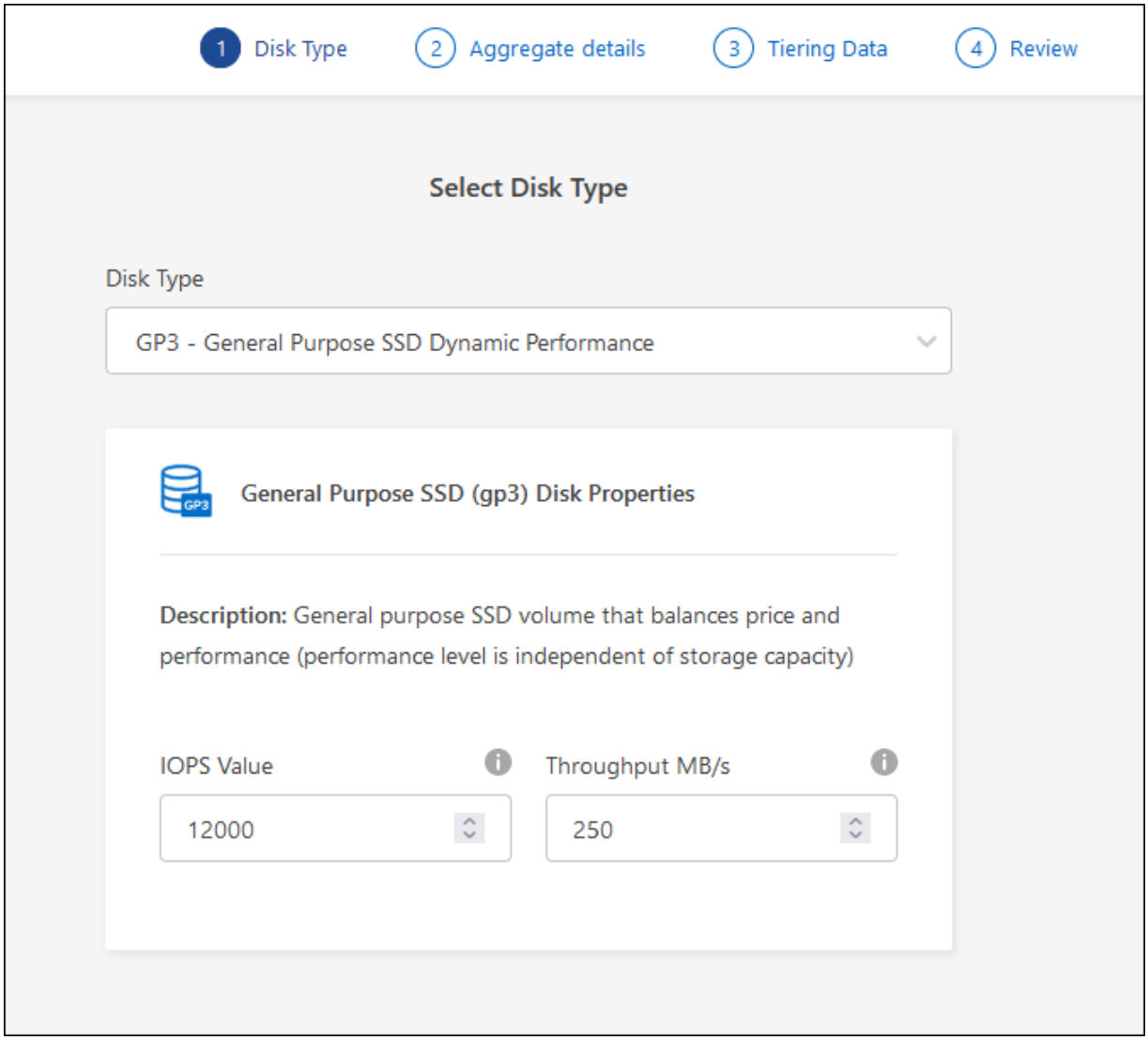
Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente dalla Console. Non dovresti eseguire queste azioni da un altro strumento di gestione. Ciò potrebbe compromettere la stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare commissioni ridondanti per il provider cloud.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
3. Nella scheda Aggregati, fare clic su **Aggiungi aggregato** e quindi specificare i dettagli per l'aggregato.

AWS

- Se ti viene chiesto di scegliere un tipo e una dimensione del disco, fai riferimento a"Pianifica la configurazione Cloud Volumes ONTAP in AWS" .
- Se ti viene chiesto di immettere la dimensione della capacità dell'aggregato, significa che stai creando un aggregato su una configurazione che supporta la funzionalità Amazon EBS Elastic Volumes. La seguente schermata mostra un esempio di un nuovo aggregato composto da dischi gp3.



"Scopri di più sul supporto per Elastic Volumes" .

Azzurro

Per assistenza sul tipo e la dimensione del disco, fare riferimento a"Pianifica la configurazione Cloud Volumes ONTAP in Azure" .

Google Cloud

Per assistenza sul tipo e la dimensione del disco, fare riferimento a"Pianifica la configurazione Cloud Volumes ONTAP in Google Cloud" .

4. Fare clic su **Aggiungi**, quindi su **Approva e acquista**.

Gestisci gli aggregati per i cluster Cloud Volumes ONTAP

Gestisci autonomamente gli aggregati aggiungendo dischi, visualizzando informazioni sugli aggregati ed eliminandoli.

> Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente dalla NetApp Console. Non dovresti eseguire queste azioni da un altro strumento di gestione. Ciò potrebbe compromettere la stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare commissioni ridondanti per il provider cloud.

Prima di iniziare

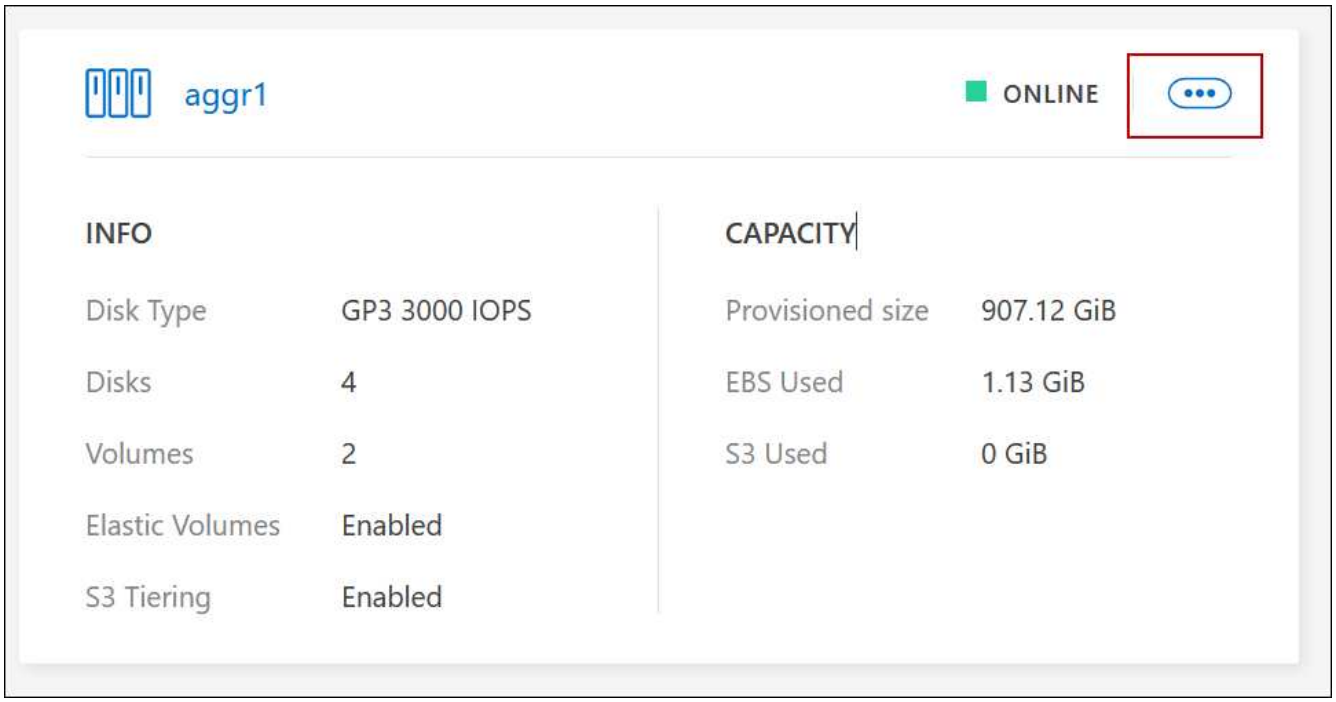
Per eliminare un aggregato, è necessario prima eliminare i volumi nell'aggregato.

Informazioni su questo compito

Se un aggregato sta esaurendo lo spazio, è possibile spostare i volumi su un altro aggregato utilizzando ONTAP System Manager.

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare doppio clic sul sistema Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
3. Dai dettagli del sistema, fare clic sulla scheda **Aggregati**.
4. Per l'aggregato richiesto, fare clic su ••• icona per le azioni di gestione.



5. Gestisci i tuoi aggregati dalle opzioni disponibili in ••• menu.

Per aggiungere dischi a un aggregato, tutti i dischi nell'aggregato devono avere le stesse dimensioni.

Per AWS, è possibile aumentare la capacità di un aggregato che supporta Amazon EBS Elastic Volumes.

1. Sotto il ••• menu, fare clic su **Aumenta capacità**.
2. Inserisci la capacità aggiuntiva che desideri aggiungere e poi clicca su **Aumenta**.

Si noti che è necessario aumentare la capacità dell'aggregato di almeno 256 GiB o del 10% delle dimensioni dell'aggregato. Ad esempio, se si dispone di un aggregato di 1,77 TiB, il 10% equivale a 181 GiB. Si tratta di una quantità inferiore a 256 GiB, quindi la dimensione dell'aggregato deve essere aumentata del minimo di 256 GiB.

Gestire la capacità aggregata di Cloud Volumes ONTAP su un agente Console

Ogni agente della console dispone di impostazioni che determinano il modo in cui gestisce la capacità aggregata per Cloud Volumes ONTAP.

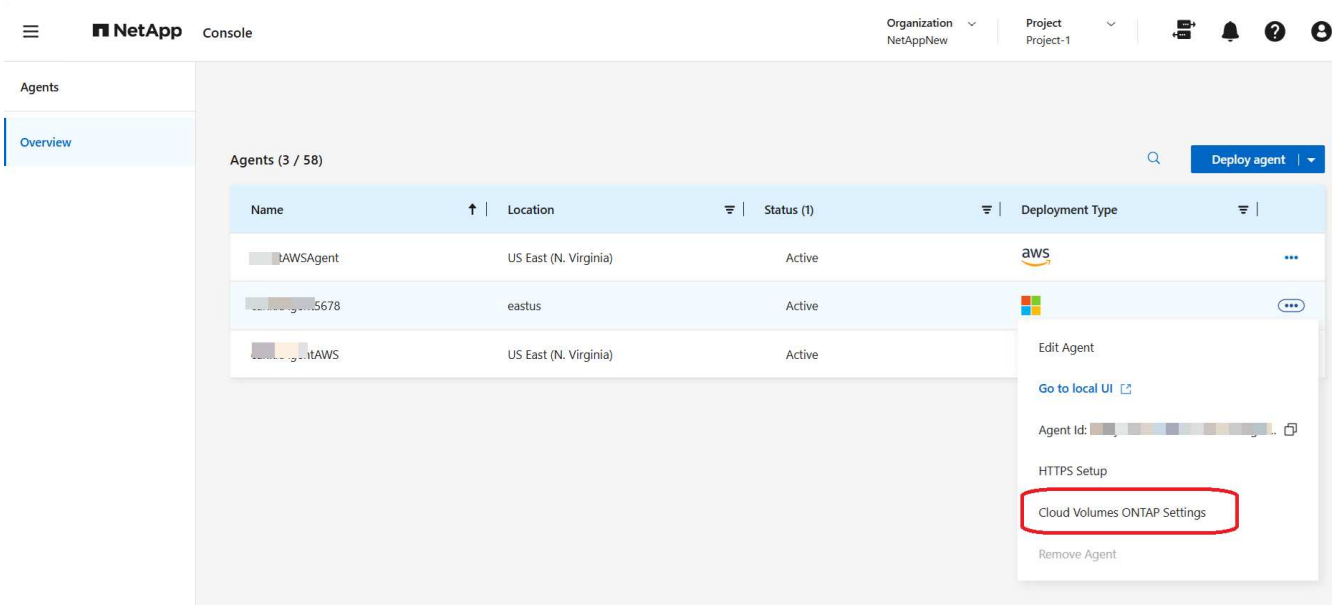
Queste impostazioni interessano tutti i sistemi Cloud Volumes ONTAP gestiti da un agente Console. Se si dispone di un altro agente Console, è possibile configurarlo in modo diverso.

Autorizzazioni richieste

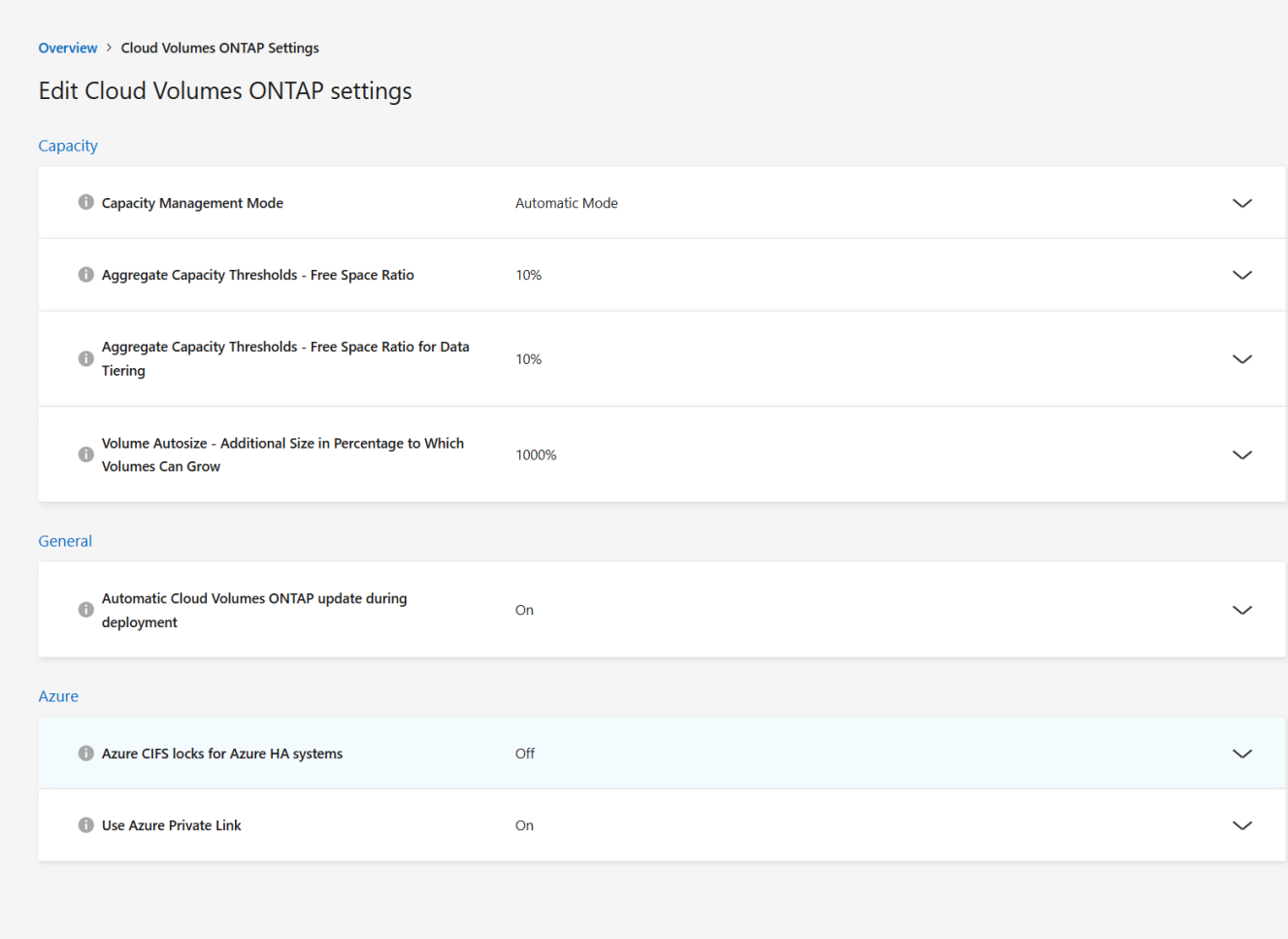
Per modificare le impostazioni Cloud Volumes ONTAP , sono necessari i privilegi di amministratore dell'organizzazione o dell'account della NetApp Console .

Passi

1. Dal riquadro di navigazione a sinistra, vai su **Amministrazione > Agenti**.
2. Fare clic su ••• icona per l'agente Console che gestisce il sistema Cloud Volumes ONTAP .
3. Selezionare *Impostazioni Cloud Volumes ONTAP *.



4. In **Capacità**, modifica una delle seguenti impostazioni:



Modalità di gestione della capacità

Scegli se la Console deve notificarti le decisioni relative alla capacità di archiviazione o se deve gestire automaticamente i requisiti di capacità per te.

"Scopri come funziona la modalità di gestione della capacità" .

Soglia di capacità aggregata - Rapporto spazio libero

Questo rapporto è un parametro chiave nelle decisioni di gestione della capacità e comprenderne l'impatto è essenziale indipendentemente dal fatto che si utilizzi una modalità di gestione della capacità automatica o manuale. Si consiglia di impostare questa soglia tenendo conto delle proprie specifiche esigenze di archiviazione e della crescita prevista per mantenere un equilibrio tra utilizzo delle risorse e costi.

In modalità manuale, se il rapporto di spazio libero su un aggregato scende al di sotto della soglia specificata, viene attivata una notifica che avvisa l'utente che è necessario adottare misure per risolvere il problema del basso rapporto di spazio libero. È importante monitorare queste notifiche e gestire manualmente la capacità aggregata per evitare interruzioni del servizio e garantire prestazioni ottimali.

Il rapporto di spazio libero è calcolato come segue: (capacità aggregata - capacità totale utilizzata sull'aggregato) / capacità aggregata

Fare riferimento a"Gestione automatica della capacità" per scoprire ora che la capacità è gestita automaticamente in Cloud Volumes ONTAP.

Soglie di capacità aggregata - Rapporto di spazio libero per la suddivisione in livelli dei dati

Definisce la quantità di spazio libero richiesta sul livello di prestazioni (dischi) quando si suddividono i dati in livelli di capacità (archiviazione di oggetti).

Il rapporto è importante per gli scenari di disaster recovery. Quando i dati vengono letti dal livello di capacità, Cloud Volumes ONTAP sposta i dati al livello di prestazioni per garantire prestazioni migliori. Se lo spazio non è sufficiente, Cloud Volumes ONTAP non può spostare i dati.

5. Fare clic su **Salva**.

Gestire le prestazioni del disco in Azure

Gestisci le prestazioni del disco Premium SSD v2 per Cloud Volumes ONTAP in Azure

È possibile ottimizzare le prestazioni Cloud Volumes ONTAP in Azure configurando i parametri IOPS e di velocità effettiva per i dischi Premium SSD v2. Questa funzionalità è disponibile solo quando Cloud Volumes ONTAP è già distribuito con il tipo di disco Azure Premium SSD v2, non durante la distribuzione iniziale. Migliorando le prestazioni, puoi sfruttare appieno la flessibilità e le capacità ad alte prestazioni dei dischi Azure Premium SSD v2.

I dischi Premium SSD v2 supportano carichi di lavoro che richiedono prestazioni rapide e affidabili con bassa latenza, IOPS elevati e throughput elevato. Regolando le impostazioni IOPS e di throughput, è possibile personalizzare le prestazioni degli aggregati nella distribuzione. Per ulteriori informazioni sui dischi Premium SSD v2, fare riferimento a "Distribuisci un disco Premium SSD v2" .

Utilizzare le API per automatizzare il processo di modifica delle impostazioni del disco Premium SSD v2. Per informazioni sull'esecuzione delle chiamate API Cloud Volumes ONTAP , fare riferimento a "La tua prima chiamata API" .

Informazioni su questo compito

- Questa funzionalità si applica alle distribuzioni Cloud Volumes ONTAP nelle singole zone di disponibilità di Azure.
- La modifica delle impostazioni del disco modifica in modo uniforme le prestazioni del gruppo o dell'aggregato RAID. Le prestazioni di tutti i dischi nell'aggregato vengono regolate allo stesso livello per garantire prestazioni uniformi nell'aggregato.
- Le modifiche interessano un singolo aggregato e non altri aggregati in un gruppo.
- I dischi Premium SSD v2 forniti automaticamente durante la distribuzione Cloud Volumes ONTAP o l'ottimizzazione della capacità nella NetApp Console, oppure aggiunti tramite le API, sono tutti idonei per la modifica.
- Il ridimensionamento del disco (modifica della capacità del disco) non è supportato.

Prima di iniziare

Prima di configurare i parametri IOPS e di throughput per i dischi Premium SSD v2, tenere presente quanto segue:

- Assicurati di aver selezionato solo dischi dati Premium SSD v2. I dischi Premium SSD v1 o i dischi di root e di avvio non sono idonei per questa modifica.
- Utilizzare le impostazioni di base preconfigurate stabilite da Cloud Volumes ONTAP durante la distribuzione come valori minimi di IOPS e throughput per le rispettive dimensioni del disco. Queste

impostazioni di base sono in linea con le caratteristiche prestazionali dell'SSD Premium v1.

- Imposta i valori IOPS e di throughput pari o superiori al valore di base minimo per le dimensioni del disco. Ad esempio, per un disco da 1 TB, impostare il valore minimo di IOPS su 5.000 e il valore minimo di throughput su 200 MBps. È possibile configurare valori superiori a questi minimi, ma non inferiori.
- Configurare i valori entro gli intervalli supportati da Premium SSD v2: IOPS tra 3000 e 80000 e throughput tra 125 e 1200 MBps.
- Assicurati che le dimensioni del disco Premium SSD v2 siano comprese nell'intervallo supportato da 500 GB a 32 TB per Cloud Volumes ONTAP in Azure. Si noti che questi limiti di dimensione differiscono dai valori minimi e massimi offerti da Azure per i dischi Premium SSD v2.

Passi

- Utilizzare la seguente chiamata API per modificare i valori degli attributi per IOPS e throughput:

  È possibile richiamare questa API al massimo quattro volte nell'arco di 24 ore.

  `PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}`

  Includi i seguenti parametri nel corpo della richiesta:

```
{
  "aggregateName": "aggr_name",
  "iops": "modified_iops_value",
  "throughput": "modified_throughput_value",
  "workingEnvironmentId": "we_id"
}
```

Dopo aver finito

Dopo che l'API restituisce una risposta che indica che l'operazione è riuscita, verifica i parametri modificati controllando i dettagli del disco nel portale di Azure per il tuo sistema Cloud Volumes ONTAP .

Informazioni correlate

- "Preparati a utilizzare l'API"
- "Flussi di lavoro Cloud Volumes ONTAP"
- "Ottieni gli identificatori richiesti"
- "Utilizzare le API REST per Cloud Volumes ONTAP"
- "Utilizzare Premium SSD v2 con le VM nel set di disponibilità"

Modificare il livello di prestazioni dei dischi SSD Premium in Cloud Volumes ONTAP in Azure

È possibile aggiornare il livello di prestazioni dei dischi gestiti Premium SSD in Cloud Volumes ONTAP in Azure tramite il portale di Azure. Si tratta di un processo manuale che prevede la modifica del livello del disco di ciascun disco Premium SSD in un livello con prestazioni più elevate. Modificando il livello di prestazioni del disco NVRAM è possibile ridurre i colli di bottiglia delle prestazioni e migliorare l'efficienza del sistema Cloud Volumes ONTAP , garantendo IOPS e capacità di throughput più elevati.

Assicurati di collaborare con il supporto NetApp per determinare se il collo di bottiglia riscontrato nel tuo ambiente è dovuto al disco NVRAM e che l'aggiornamento del livello risolve il problema.

Informazioni su questo compito

- Per impostazione predefinita, Cloud Volumes ONTAP in Azure distribuisce dischi SSD Premium per NVRAM nel livello P20. Il livello P20 offre prestazioni bilanciate adatte alla maggior parte dei carichi di lavoro. Tuttavia, se il carico di lavoro richiede prestazioni più elevate, è possibile aggiornare il disco NVRAM a un livello superiore, ad esempio P30.

  Attualmente è possibile aggiornare un disco NVRAM dal livello P20 al livello P30 solo tramite il portale di Azure.

- Non si modifica la dimensione del disco. Continua a essere di 512 GB. Questa procedura modifica solo il livello di prestazioni del disco.

Prima di iniziare

- Valutare attentamente la necessità di questa modifica, perché l'aggiornamento del disco NVRAM a un livello di prestazioni più elevato comporta costi aggiuntivi.
- La versione Cloud Volumes ONTAP deve essere 9.11.1 o successiva. Per le versioni precedenti, è possibile effettuare l'aggiornamento alla versione 9.11.1 o successiva oppure inviare una richiesta di variazione della policy sulle funzionalità (FPVR) con il supporto NetApp .

Passi

Questo scenario presuppone che ci siano due nodi `node01` E `node02` nell'implementazione ad alta disponibilità (HA) di Cloud Volumes ONTAP . Utilizzare il portale di Azure per aggiornare il livello.

1. Esegui questo comando per creare `node1` il nodo attivo. Failover manuale `node02`.

   ```
   storage failover takeover -ofnode <Node02>
   ```

2. Sign in al portale di Azure.
3. Una volta completata l'acquisizione, passare all'istanza della VM per `node02`e fare clic sul pulsante **Stop** per disattivarlo.
4. Passare al gruppo di risorse per `node02` e dall'elenco dei dischi, seleziona il disco NVRAM per cambiare livello.
5. Seleziona **Dimensioni + Prestazioni**.
6. Nel menu a discesa **Livello di prestazioni**, seleziona `P30 - 5000 IOPS, 200MB/s`.
7. Seleziona **Ridimensiona**.
8. Accendi il `node02` esempio.
9. Controllare la console seriale di Azure finché non viene visualizzato il messaggio: `waiting for giveback`.
10. Esegui questo comando per restituire `node02`:

    ```
    storage failover giveback -ofnode <Node02>
    ```

11. Ripetere questi passaggi su `node01` fare `node02` rilevare `node01`, in modo da poter aggiornare il livello del disco NVRAM per `node01`.

Dopo aver finito

Dopo aver attivato entrambi i nodi, verificare i parametri modificati controllando i dettagli del disco nel portale di Azure per il sistema Cloud Volumes ONTAP .

Informazioni correlate

- Documentazione di Azure: "Cambia il tuo livello di prestazioni senza tempi di inattività"
- Base di conoscenza per il team di supporto: "Come aggiornare il livello di prestazioni del disco NVRAM in Azure CVO"
- "Aggiorna le versioni del software Cloud Volumes ONTAP"

Amministrazione della VM di archiviazione

Gestisci le VM di archiviazione per Cloud Volumes ONTAP

Una VM di archiviazione è una macchina virtuale in esecuzione all'interno di ONTAP che fornisce servizi di archiviazione e dati ai tuoi client. Potresti conoscerlo come *SVM* o *vserver*. Per impostazione predefinita, Cloud Volumes ONTAP è configurato con una VM di archiviazione, ma alcune configurazioni supportano VM di archiviazione aggiuntive.

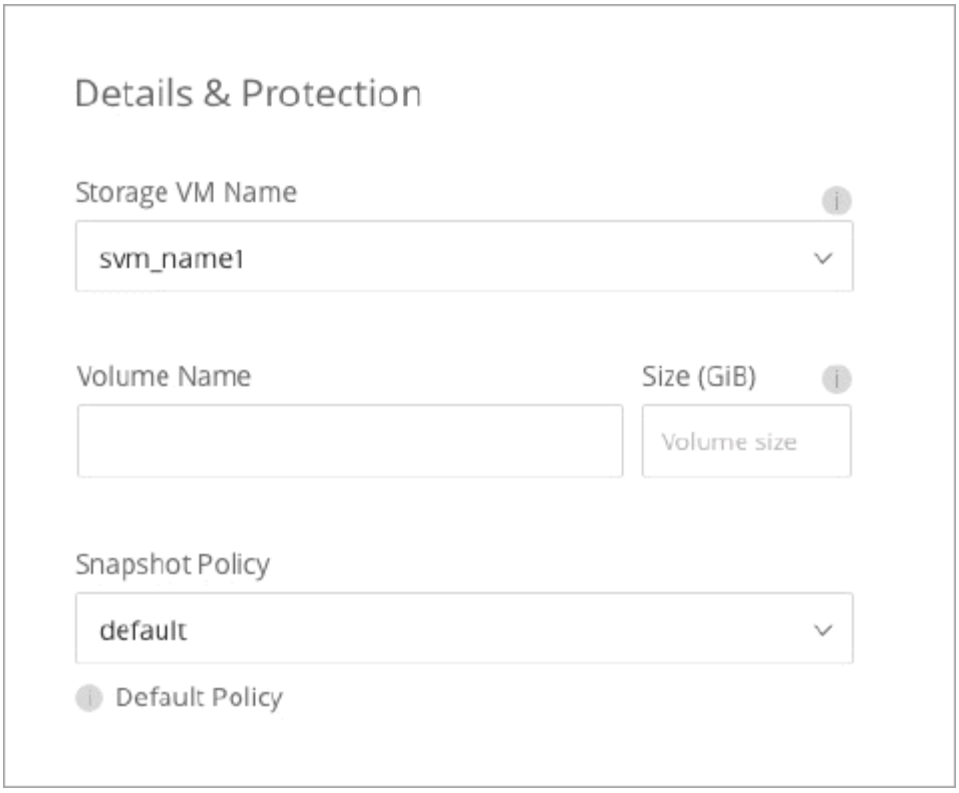
Numero supportato di VM di archiviazione

Con determinate configurazioni sono supportate più VM di archiviazione. Vai al "Note sulla versione Cloud Volumes ONTAP" per verificare il numero supportato di VM di archiviazione per la tua versione di Cloud Volumes ONTAP.

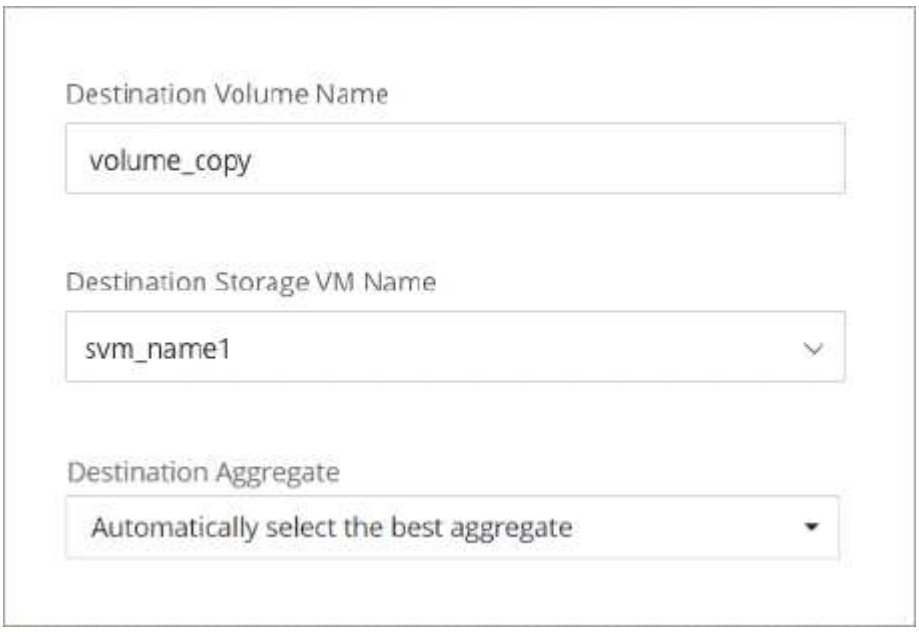
Lavora con più VM di storage

La NetApp Console supporta qualsiasi VM di storage aggiuntiva creata da ONTAP System Manager o da ONTAP CLI.

Ad esempio, l'immagine seguente mostra come scegliere una VM di archiviazione quando si crea un volume.



L'immagine seguente mostra come scegliere una VM di archiviazione quando si replica un volume su un altro sistema.



Modificare il nome della VM di archiviazione predefinita

La console assegna automaticamente un nome alla singola VM di archiviazione creata per Cloud Volumes ONTAP. Da ONTAP System Manager, dalla CLI ONTAP o dall'API, è possibile modificare il nome della VM di archiviazione se si hanno standard di denominazione rigorosi. Ad esempio, potresti voler far corrispondere il nome assegnato alle VM di archiviazione per i tuoi cluster ONTAP .

Gestisci le VM di archiviazione dati per Cloud Volumes ONTAP in AWS

Una VM di archiviazione è una macchina virtuale in esecuzione all'interno di ONTAP che fornisce servizi di archiviazione e dati ai tuoi client. Potresti conoscerlo come *SVM* o *vserver*. Per impostazione predefinita, Cloud Volumes ONTAP è configurato con una VM di archiviazione, ma alcune configurazioni supportano VM di archiviazione aggiuntive.

Per creare ulteriori VM di archiviazione per la distribuzione dei dati, è necessario allocare indirizzi IP in AWS e quindi eseguire comandi ONTAP in base alla configurazione Cloud Volumes ONTAP .

Numero supportato di VM di archiviazione

A partire dalla versione 9.7, sono supportate più VM di storage con configurazioni specifiche Cloud Volumes ONTAP . Vai al "Note sulla versione Cloud Volumes ONTAP" per verificare il numero supportato di VM di archiviazione per la tua versione di Cloud Volumes ONTAP.

Tutte le altre configurazioni Cloud Volumes ONTAP supportano una VM di storage per la gestione dei dati e una VM di storage di destinazione utilizzata per il disaster recovery. È possibile attivare la VM di archiviazione di destinazione per l'accesso ai dati in caso di interruzione della VM di archiviazione di origine.

Verifica i limiti per la tua configurazione

Ogni istanza EC2 supporta un numero massimo di indirizzi IPv4 privati per interfaccia di rete. È necessario verificare il limite prima di allocare indirizzi IP in AWS per la nuova VM di archiviazione.

Passi

1. Vai al "Sezione Limiti di archiviazione nelle Note sulla versione Cloud Volumes ONTAP" .
2. Identifica il numero massimo di indirizzi IP per interfaccia per il tuo tipo di istanza.
3. Prendi nota di questo numero perché ti servirà nella prossima sezione quando assegnerai gli indirizzi IP in AWS.

Assegnare indirizzi IP in AWS

Prima di creare LIF per la nuova VM di archiviazione, è necessario assegnare indirizzi IPv4 privati alla porta e0a in AWS.

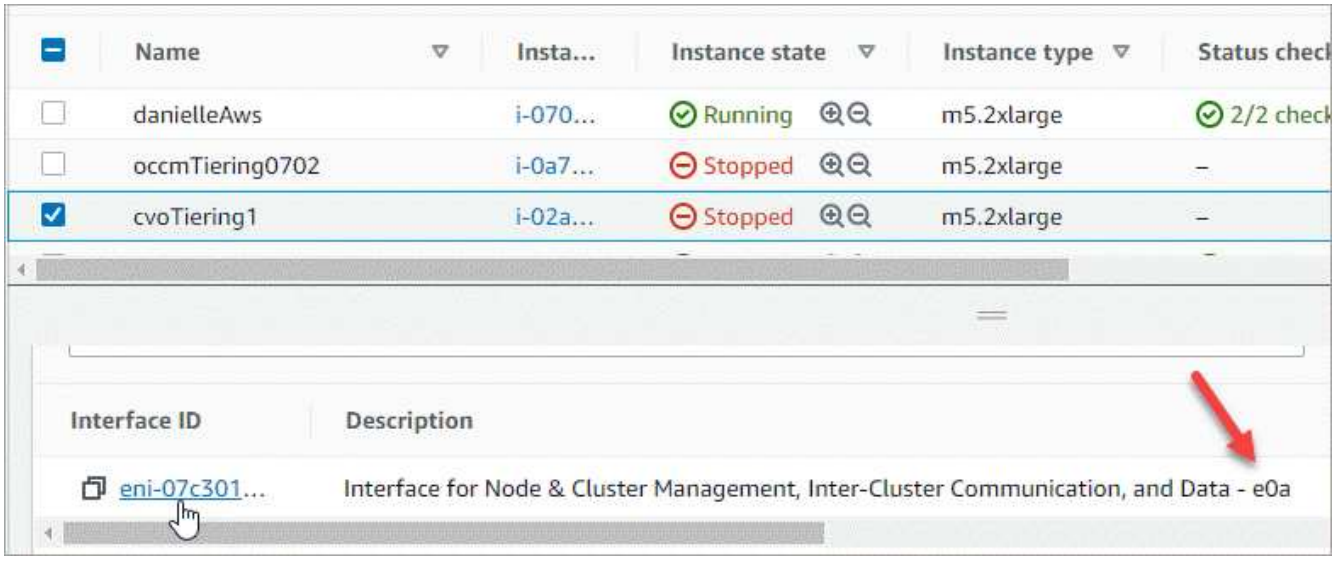
Si noti che un LIF di gestione opzionale per una VM di storage richiede un indirizzo IP privato su un sistema a nodo singolo e su una coppia HA in una singola AZ. Questo LIF di gestione fornisce una connessione a strumenti di gestione come SnapCenter.

Passi

1. Accedi ad AWS e apri il servizio EC2.
2. Selezionare l'istanza Cloud Volumes ONTAP e fare clic su **Networking**.

   Se si sta creando una VM di archiviazione su una coppia HA, selezionare il nodo 1.

3. Scorrere verso il basso fino a **Interfacce di rete** e fare clic su **ID interfaccia** per la porta e0a.



4. Selezionare l'interfaccia di rete e fare clic su **Azioni > Gestisci indirizzi IP**.
5. Espandi l'elenco degli indirizzi IP per e0a.
6. Verificare gli indirizzi IP:
   a. Contare il numero di indirizzi IP assegnati per confermare che la porta abbia spazio per IP aggiuntivi.

      Nella sezione precedente di questa pagina dovresti aver identificato il numero massimo di indirizzi IP supportati per interfaccia.

   b. Facoltativo: accedere alla CLI ONTAP per Cloud Volumes ONTAP ed eseguire **network interface show** per confermare che ciascuno di questi indirizzi IP sia in uso.

      Se un indirizzo IP non è in uso, è possibile utilizzarlo con la nuova VM di archiviazione.
7. Tornando alla console AWS, fai clic su **Assegna nuovo indirizzo IP** per assegnare indirizzi IP aggiuntivi in base alla quantità necessaria per la nuova VM di archiviazione.
   - sistema a nodo singolo: è necessario un IP privato secondario non utilizzato.

     Se si desidera creare un LIF di gestione sulla VM di archiviazione, è necessario un IP privato secondario facoltativo.

   - Coppia HA in una singola AZ: è richiesto un IP privato secondario non utilizzato sul nodo 1.

     Se si desidera creare un LIF di gestione sulla VM di archiviazione, è necessario un IP privato secondario facoltativo.

   - Coppia HA in più AZ: è richiesto un IP privato secondario non utilizzato su ciascun nodo.
8. Se si sta assegnando l'indirizzo IP su una coppia HA in una singola AZ, abilitare **Consenti la riassegnazione degli indirizzi IPv4 privati secondari**.
9. Fare clic su **Salva**.
10. Se si dispone di una coppia HA in più AZ, sarà necessario ripetere questi passaggi per il nodo 2.

Crea una VM di archiviazione su un sistema a nodo singolo

Questi passaggi creano una nuova VM di storage su un sistema a nodo singolo. È necessario un indirizzo IP privato per creare un LIF NAS e un altro indirizzo IP privato facoltativo se si desidera creare un LIF di gestione.

Passi

1. Creare la VM di archiviazione e un percorso verso la VM di archiviazione.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Creare un NAS LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

   Dove *private_ip_x* è un IP privato secondario non utilizzato su e0a.

3. Facoltativo: creare un LIF di gestione delle VM di archiviazione.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

   Dove *private_ip_y* è un altro IP privato secondario non utilizzato su e0a.

4. Assegnare uno o più aggregati alla VM di archiviazione.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Questo passaggio è necessario perché la nuova VM di archiviazione deve avere accesso ad almeno un aggregato prima di poter creare volumi sulla VM di archiviazione.

Crea una VM di archiviazione su una coppia HA in una singola AZ

Questi passaggi creano una nuova VM di archiviazione su una coppia HA in una singola AZ. Per creare un LIF NAS è necessario un indirizzo IP privato, mentre se si desidera creare un LIF di gestione è necessario un altro indirizzo IP privato facoltativo.

Entrambi questi LIF vengono allocati sul nodo 1. In caso di guasti, gli indirizzi IP privati possono spostarsi tra i nodi.

Passi

1. Creare la VM di archiviazione e un percorso verso la VM di archiviazione.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Creare un NAS LIF sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Dove *private_ip_x* è un IP privato secondario non utilizzato su e0a di cvo-node1. Questo indirizzo IP può essere riposizionato nell'e0a di cvo-node2 in caso di acquisizione perché la policy di servizio default-data-files indica che gli IP possono migrare al nodo partner.

3. Facoltativo: creare un LIF di gestione della VM di archiviazione sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Dove *private_ip_y* è un altro IP privato secondario non utilizzato su e0a.

4. Assegnare uno o più aggregati alla VM di archiviazione.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Questo passaggio è necessario perché la nuova VM di archiviazione deve avere accesso ad almeno un aggregato prima di poter creare volumi sulla VM di archiviazione.

5. Se si esegue Cloud Volumes ONTAP 9.11.1 o versione successiva, modificare i criteri del servizio di rete per la VM di archiviazione.

La modifica dei servizi è necessaria perché garantisce che Cloud Volumes ONTAP possa utilizzare iSCSI LIF per le connessioni di gestione in uscita.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Creare una VM di archiviazione su una coppia HA in più AZ

Questi passaggi creano una nuova VM di archiviazione su una coppia HA in più AZ.

Per un LIF NAS è richiesto un indirizzo IP *floating*, mentre è facoltativo per un LIF di gestione. Questi indirizzi IP mobili non richiedono l'assegnazione di IP privati in AWS. Al contrario, gli IP mobili vengono configurati automaticamente nella tabella di routing AWS per puntare all'ENI di un nodo specifico nella stessa VPC.

Affinché gli IP flottanti funzionino con ONTAP, è necessario configurare un indirizzo IP privato su ogni VM di storage su ciascun nodo. Ciò si riflette nei passaggi seguenti in cui viene creato un iSCSI LIF sul nodo 1 e sul nodo 2.

Passi

1. Creare la VM di archiviazione e un percorso verso la VM di archiviazione.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Creare un NAS LIF sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - L'indirizzo IP mobile deve essere esterno ai blocchi CIDR per tutte le VPC nella regione AWS in cui si distribuisce la configurazione HA. 192.168.209.27 è un esempio di indirizzo IP mobile. "Scopri di più sulla scelta di un indirizzo IP flottante" .
   - `-service-policy default-data-files`indica che gli IP possono migrare al nodo partner.

3. Facoltativo: creare un LIF di gestione della VM di archiviazione sul nodo 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Creare un iSCSI LIF sul nodo 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - Questo iSCSI LIF è necessario per supportare la migrazione LIF degli IP mobili nella VM di archiviazione. Non deve essere necessariamente un iSCSI LIF, ma non può essere configurato per la migrazione tra nodi.
   - `-service-policy default-data-block`indica che un indirizzo IP non migra tra i nodi.
   - *private_ip* è un indirizzo IP privato secondario non utilizzato su eth0 (e0a) di cvo_node1.

5. Creare un iSCSI LIF sul nodo 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- Questo iSCSI LIF è necessario per supportare la migrazione LIF degli IP mobili nella VM di archiviazione. Non deve essere necessariamente un iSCSI LIF, ma non può essere configurato per la migrazione tra nodi.
- `-service-policy default-data-block`indica che un indirizzo IP non migra tra i nodi.
- *private_ip* è un indirizzo IP privato secondario non utilizzato su eth0 (e0a) di cvo_node2.

6. Assegnare uno o più aggregati alla VM di archiviazione.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Questo passaggio è necessario perché la nuova VM di archiviazione deve avere accesso ad almeno un aggregato prima di poter creare volumi sulla VM di archiviazione.

7. Se si esegue Cloud Volumes ONTAP 9.11.1 o versione successiva, modificare i criteri del servizio di rete per la VM di archiviazione.

La modifica dei servizi è necessaria perché garantisce che Cloud Volumes ONTAP possa utilizzare iSCSI LIF per le connessioni di gestione in uscita.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Gestisci le VM di archiviazione per il servizio dati per Cloud Volumes ONTAP in Azure

Una VM di archiviazione è una macchina virtuale in esecuzione all'interno di ONTAP che fornisce servizi di archiviazione e dati ai tuoi client. Potresti conoscerlo come *SVM* o *vserver*. Per impostazione predefinita, Cloud Volumes ONTAP è configurato con una VM di archiviazione, ma è possibile creare VM di archiviazione aggiuntive quando si esegue Cloud Volumes ONTAP in Azure.

Per creare e gestire ulteriori VM di archiviazione dati in Azure, è necessario utilizzare le API. Questo perché le API automatizzano il processo di creazione delle VM di archiviazione e di configurazione delle interfacce di rete richieste. Durante la creazione delle VM di storage, la NetApp Console configura i servizi LIF richiesti, nonché un LIF iSCSI necessario per le comunicazioni SMB/CIFS in uscita dalla VM di storage.

Per informazioni sull'esecuzione delle chiamate API Cloud Volumes ONTAP , fare riferimento a "La tua prima

chiamata API" .

Numero supportato di VM di archiviazione

A partire da Cloud Volumes ONTAP 9.9.0, in base alla licenza, sono supportate più VM di archiviazione con configurazioni specifiche. Fare riferimento al "Note sulla versione Cloud Volumes ONTAP" per verificare il numero supportato di VM di archiviazione per la tua versione di Cloud Volumes ONTAP.

Tutte le versioni di Cloud Volumes ONTAP precedenti alla 9.9.0 supportano una VM di archiviazione dati e una VM di archiviazione di destinazione utilizzata per il ripristino di emergenza. È possibile attivare la VM di archiviazione di destinazione per l'accesso ai dati in caso di interruzione della VM di archiviazione di origine.

Creare una VM di archiviazione

In base alla configurazione e al tipo di licenza, è possibile creare più VM di archiviazione su un sistema a nodo singolo o in una configurazione ad alta disponibilità (HA) utilizzando le API per la NetApp Console.

Informazioni su questo compito

Quando si creano VM di archiviazione utilizzando le API, insieme alla configurazione delle interfacce di rete richieste, la Console modifica anche `default-data-files` policy sulle VM di archiviazione dati rimuovendo i seguenti servizi dal LIF dati NAS e aggiungendoli al LIF dati iSCSI utilizzato per le connessioni di gestione in uscita:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Prima di iniziare

L'agente della console richiede autorizzazioni specifiche per creare VM di archiviazione per Cloud Volumes ONTAP. Le autorizzazioni richieste sono incluse in "le policy fornite da NetApp" .

sistema a nodo singolo

Utilizzare la seguente chiamata API per creare una storage VM su un sistema a nodo singolo.

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

Includi i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

coppia HA

Utilizzare la seguente chiamata API per creare una VM di archiviazione su una coppia HA:

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

Includi i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

Gestisci le VM di storage su sistemi a nodo singolo e coppia HA

Utilizzando le API, è possibile rinominare ed eliminare le VM di storage sia nelle configurazioni a nodo singolo che in quelle HA.

Prima di iniziare

L'agente Console richiede autorizzazioni specifiche per gestire le VM di archiviazione per Cloud Volumes ONTAP. Le autorizzazioni richieste sono incluse in "le policy fornite da NetApp" .

Rinominare una VM di archiviazione

Per rinominare una VM di archiviazione, è necessario fornire come parametri i nomi della VM di archiviazione esistente e della nuova VM di archiviazione.

Passi

- Utilizzare la seguente chiamata API per rinominare una storage VM su un sistema a nodo singolo:

  ```
  PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  Includi i seguenti parametri nel corpo della richiesta:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Utilizzare la seguente chiamata API per rinominare una VM di archiviazione su una coppia HA:

  ```
  PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
  ```

  Includi i seguenti parametri nel corpo della richiesta:

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

Elimina una VM di archiviazione

In una configurazione a nodo singolo o HA, è possibile rimuovere una VM di archiviazione se non dispone di volumi attivi.

Passi

- Utilizzare la seguente chiamata API per eliminare una storage VM su un sistema a nodo singolo:

  `DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}`

- Utilizzare la seguente chiamata API per eliminare una VM di archiviazione su una coppia HA:

  `DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}`

Informazioni correlate

- "Preparati a utilizzare l'API"
- "Flussi di lavoro Cloud Volumes ONTAP"
- "Ottieni gli identificatori richiesti"
- "Utilizzare le API REST per NetApp Console"

Gestisci le VM di archiviazione dati per Cloud Volumes ONTAP in Google Cloud

Una VM di archiviazione è una macchina virtuale in esecuzione all'interno di ONTAP che fornisce servizi di archiviazione e dati ai tuoi client. Potresti conoscerlo come *SVM* o *vserver*. Per impostazione predefinita, Cloud Volumes ONTAP è configurato con una VM di archiviazione, ma alcune configurazioni supportano VM di archiviazione aggiuntive.

Per creare e gestire ulteriori VM di archiviazione dati in Google Cloud, è necessario utilizzare le API. Questo perché le API automatizzano il processo di creazione delle VM di archiviazione e di configurazione delle interfacce di rete richieste. Durante la creazione delle VM di storage, la NetApp Console configura i servizi LIF richiesti, nonché un LIF iSCSI necessario per le comunicazioni SMB/CIFS in uscita dalla VM di storage.

Per informazioni sull'esecuzione delle chiamate API Cloud Volumes ONTAP , fare riferimento a "La tua prima chiamata API" .

Numero supportato di VM di archiviazione

A partire da Cloud Volumes ONTAP 9.11.1, in base alla licenza, sono supportate più VM di archiviazione con configurazioni specifiche. Fare riferimento al "Note sulla versione Cloud Volumes ONTAP" per verificare il numero supportato di VM di archiviazione per la tua versione di Cloud Volumes ONTAP.

Tutte le versioni di Cloud Volumes ONTAP precedenti alla 9.11.1 supportano una VM di archiviazione dati e una VM di archiviazione di destinazione utilizzata per il ripristino di emergenza. È possibile attivare la VM di

archiviazione di destinazione per l'accesso ai dati in caso di interruzione della VM di archiviazione di origine.

Creare una VM di archiviazione

In base alla configurazione e al tipo di licenza, puoi creare più storage VM su un sistema a nodo singolo o in una configurazione ad alta disponibilità (coppia HA) utilizzando le API.

Informazioni su questo compito

Quando si creano VM di archiviazione utilizzando le API, insieme alla configurazione delle interfacce di rete richieste, la Console modifica anche `default-data-files` policy sulle VM di archiviazione dati rimuovendo i seguenti servizi dal LIF dati NAS e aggiungendoli al LIF dati iSCSI utilizzato per le connessioni di gestione in uscita:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Prima di iniziare

L'agente della console richiede autorizzazioni specifiche per creare VM di archiviazione per coppie Cloud Volumes ONTAP HA. Le autorizzazioni richieste sono incluse in "le policy fornite da NetApp" .

sistema a nodo singolo

Utilizzare la seguente chiamata API per creare una storage VM su un sistema a nodo singolo.

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

Includi i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

coppia HA

Utilizzare la seguente chiamata API per creare una VM di archiviazione su una coppia HA:

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

Includi i seguenti parametri nel corpo della richiesta:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

Gestire le VM di archiviazione

Utilizzando le API, è possibile rinominare ed eliminare le VM di storage sia nelle configurazioni a nodo singolo che in quelle HA.

Prima di iniziare

L'agente della console richiede autorizzazioni specifiche per gestire le VM di archiviazione per le coppie Cloud Volumes ONTAP HA. Le autorizzazioni richieste sono incluse in "le policy fornite da NetApp" .

Rinominare una VM di archiviazione

Per rinominare una VM di archiviazione, è necessario fornire come parametri i nomi della VM di archiviazione esistente e della nuova VM di archiviazione.

Passi

- Utilizzare la seguente chiamata API per rinominare una storage VM su un sistema a nodo singolo:

  `PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

  Includi i seguenti parametri nel corpo della richiesta:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Utilizzare la seguente chiamata API per rinominare una VM di archiviazione su una coppia HA:

  `PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm`

  Includi i seguenti parametri nel corpo della richiesta:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

Elimina una VM di archiviazione

In una configurazione a nodo singolo o HA, è possibile rimuovere una VM di archiviazione se non dispone di volumi attivi.

Passi

- Utilizzare la seguente chiamata API per eliminare una storage VM su un sistema a nodo singolo:

  ```
  DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

- Utilizzare la seguente chiamata API per eliminare una VM di archiviazione su una coppia HA:

  ```
  DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

Informazioni correlate

- "Preparati a utilizzare l'API"
- "Flussi di lavoro Cloud Volumes ONTAP"
- "Ottieni gli identificatori richiesti"
- "Utilizzare le API REST per la NetApp Console"

Configurare il disaster recovery della VM di archiviazione per Cloud Volumes ONTAP

La NetApp Console non offre supporto per la configurazione o l'orchestrazione per il ripristino di emergenza delle VM di archiviazione (SVM). Per eseguire queste attività, utilizzare ONTAP System Manager o ONTAP CLI.

Se si imposta la replica SVM SnapMirror tra due sistemi Cloud Volumes ONTAP, la replica deve essere eseguita tra due sistemi a coppia HA o due sistemi a nodo singolo. Non è possibile impostare la replica SVM SnapMirror tra una coppia HA e un sistema a nodo singolo.

Per le istruzioni di ONTAP CLI, fare riferimento ai seguenti documenti.

- "Guida rapida alla preparazione al ripristino di emergenza SVM"
- "Guida rapida al ripristino di emergenza SVM"

Sicurezza e crittografia dei dati

Crittografa i volumi su Cloud Volumes ONTAP con le soluzioni di crittografia NetApp

Cloud Volumes ONTAP supporta NetApp Volume Encryption (NVE) e NetApp Aggregate Encryption (NAE). NVE e NAE sono soluzioni basate su software che consentono la crittografia dei dati a riposo dei volumi conforme allo standard FIPS 140-2. "Scopri di più su queste soluzioni di crittografia" .

Sia NVE che NAE sono supportati da un gestore di chiavi esterno.

] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[

Gestisci le chiavi di crittografia Cloud Volumes ONTAP con AWS Key Management Service

Puoi usare"Servizio di gestione delle chiavi (KMS) di AWS" per proteggere le chiavi di crittografia ONTAP in un'applicazione distribuita su AWS.

La gestione delle chiavi con AWS KMS può essere abilitata tramite la CLI o l'API REST ONTAP .

Quando si utilizza il KMS, tenere presente che per impostazione predefinita viene utilizzato il LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi cloud. Per comunicare con i servizi di autenticazione di AWS viene utilizzata una rete di gestione dei nodi. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.12.0 o successiva
- È necessario aver installato la licenza Volume Encryption (VE) e
- È necessario aver installato la licenza Multi-tenant Encryption Key Management (MTEKM).
- Devi essere un amministratore del cluster o SVM
- Devi avere un abbonamento AWS attivo

È possibile configurare le chiavi solo per una SVM dati.

Configurazione

AWS

1. Devi creare un"concessione" per la chiave AWS KMS che verrà utilizzata dal ruolo IAM che gestisce la crittografia. Il ruolo IAM deve includere una policy che consenta le seguenti operazioni:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`Per creare una sovvenzione, fare riferimento a"Documentazione AWS" .
2. "Aggiungere un criterio al ruolo IAM appropriato."La politica dovrebbe sostenere l' `DescribeKey` , `Encrypt` , E `Decrypt` operazioni.

Cloud Volumes ONTAP

1. Passa al tuo ambiente Cloud Volumes ONTAP .
2. Passa al livello di privilegio avanzato:
   `set -privilege advanced`
3. Abilitare il gestore delle chiavi AWS:
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando richiesto, immettere la chiave segreta.
5. Verifica che AWS KMS sia stato configurato correttamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Azure Key Vault

È possibile utilizzare Azure Key Vault (AKV) per proteggere le chiavi di crittografia ONTAP in un'applicazione distribuita in Azure. Fare riferimento al"Documentazione Microsoft" .

AKV può essere utilizzato per proteggere le chiavi NetApp Volume Encryption (NVE) solo per le SVM di dati. Per ulteriori informazioni, fare riferimento al "Documentazione ONTAP" .

La gestione delle chiavi con AKV può essere abilitata tramite la CLI o l'API REST ONTAP .

Quando si utilizza AKV, tenere presente che per impostazione predefinita viene utilizzato un LIF SVM dati per comunicare con l'endpoint di gestione delle chiavi cloud. Per comunicare con i servizi di autenticazione del provider cloud (login.microsoftonline.com) viene utilizzata una rete di gestione dei nodi. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Cloud Volumes ONTAP deve eseguire la versione 9.10.1 o successiva
- Licenza Volume Encryption (VE) installata (la licenza NetApp Volume Encryption viene installata automaticamente su ogni sistema Cloud Volumes ONTAP registrato presso il supporto NetApp)
- È necessario disporre di una licenza Multi-tenant Encryption Key Management (MT_EK_MGMT)
- Devi essere un amministratore del cluster o SVM
- Un abbonamento Azure attivo

Limitazioni

- AKV può essere configurato solo su un SVM dati
- NAE non può essere utilizzato con AKV. NAE richiede un server KMIP supportato esternamente.
- I nodi Cloud Volumes ONTAP interrogano AKV ogni 15 minuti per confermare l'accessibilità e la disponibilità delle chiavi. Questo periodo di polling non è configurabile e, dopo quattro errori consecutivi nel tentativo di polling (per un totale di 1 ora), i volumi vengono messi offline.

Processo di configurazione

I passaggi descritti descrivono come registrare la configurazione di Cloud Volumes ONTAP con Azure e come creare un Azure Key Vault e le relative chiavi. Se hai già completato questi passaggi, assicurati di avere le impostazioni di configurazione corrette, in particolare inCreare un Azure Key Vault , e poi procedere aConfigurazione Cloud Volumes ONTAP .

- Registrazione dell'applicazione Azure
- Crea il segreto client di Azure
- Creare un Azure Key Vault
- Crea chiave di crittografia
- Creare un endpoint di Azure Active Directory (solo HA)
- Configurazione Cloud Volumes ONTAP

Registrazione dell'applicazione Azure

1. Devi prima registrare la tua applicazione nella sottoscrizione di Azure che desideri che Cloud Volumes ONTAP utilizzi per accedere ad Azure Key Vault. Nel portale di Azure, seleziona **Registrazioni app**.

2. Selezionare **Nuova registrazione**.
3. Fornisci un nome per la tua applicazione e seleziona un tipo di applicazione supportato. Per l'utilizzo di Azure Key Vault è sufficiente il tenant singolo predefinito. Seleziona **Registrati**.
4. Nella finestra Panoramica di Azure, seleziona l'applicazione che hai registrato. Copiare l'**ID applicazione (client)** e l'**ID directory (tenant)** in una posizione sicura. Saranno richiesti più avanti nel processo di registrazione.

Crea il segreto client di Azure

1. Nel portale di Azure per la registrazione dell'app Azure Key Vault, seleziona il riquadro **Certificati e segreti**.
2. Seleziona **Nuovo segreto client**. Inserisci un nome significativo per il tuo segreto client. NetApp consiglia un periodo di scadenza di 24 mesi; tuttavia, le tue specifiche policy di governance del cloud potrebbero richiedere un'impostazione diversa.
3. Fare clic su **Aggiungi** per creare il segreto client. Copiare la stringa segreta elencata nella colonna **Valore** e memorizzarla in un luogo sicuro per un utilizzo successivo inConfigurazione Cloud Volumes ONTAP . Il valore segreto non verrà più visualizzato dopo aver abbandonato la pagina.

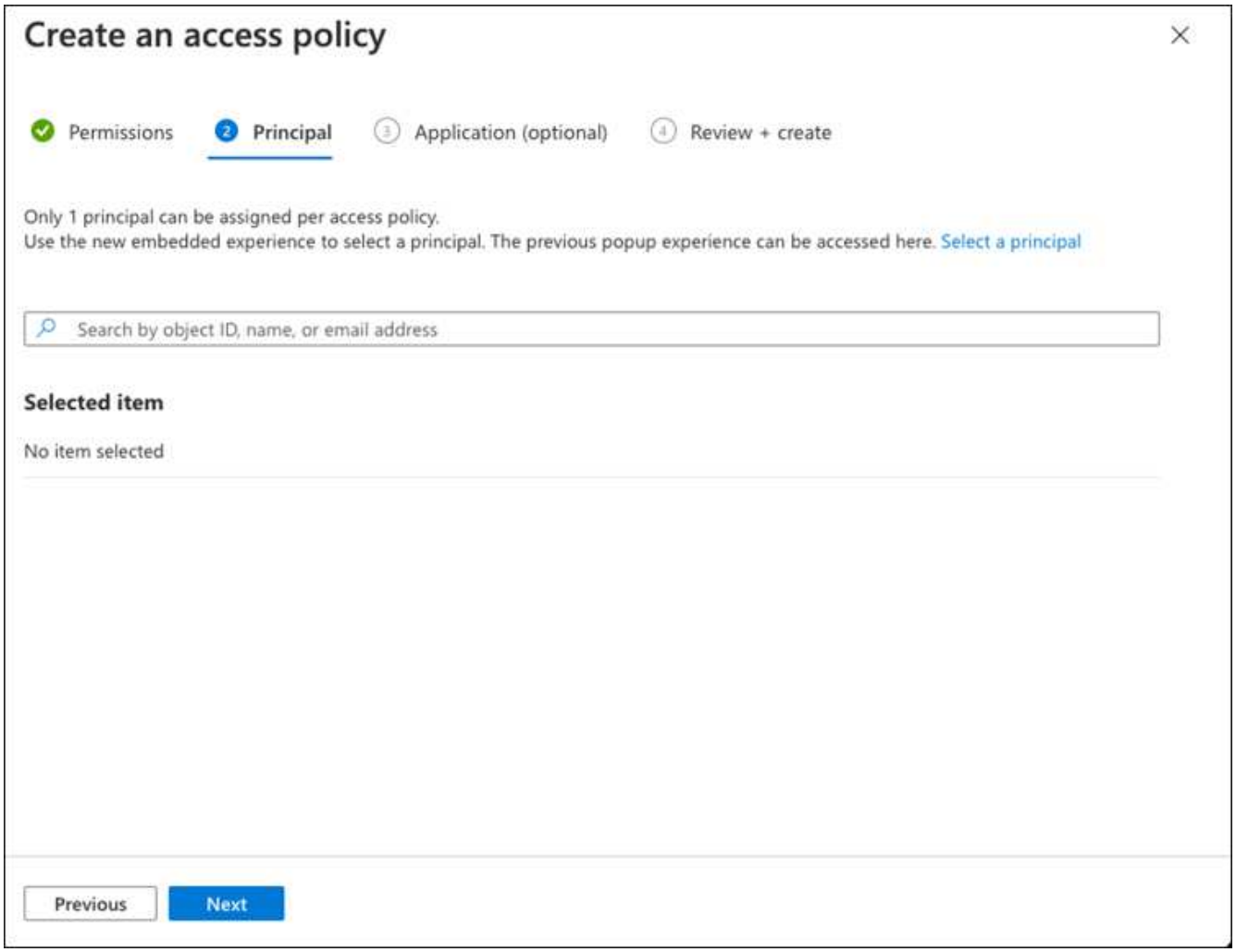
Creare un Azure Key Vault

1. Se disponi di un Azure Key Vault esistente, puoi connetterlo alla configurazione Cloud Volumes ONTAP ; tuttavia, devi adattare i criteri di accesso alle impostazioni in questo processo.
2. Nel portale di Azure, passare alla sezione **Key Vault**.
3. Fare clic su **+Crea** e immettere le informazioni richieste, tra cui gruppo di risorse, regione e livello di prezzo. Inoltre, immettere il numero di giorni per cui conservare i vault eliminati e selezionare **Abilita protezione di eliminazione** sul vault delle chiavi.
4. Selezionare **Avanti** per scegliere una policy di accesso.
5. Selezionare le seguenti opzioni:
   a. In **Configurazione di accesso**, seleziona **Criterio di accesso al Vault**.
   b. In **Accesso alle risorse**, seleziona **Azure Disk Encryption per la crittografia del volume**.
6. Selezionare **+Crea** per aggiungere un criterio di accesso.
7. In **Configura da un modello**, fai clic sul menu a discesa e seleziona il modello **Gestione chiavi, segreti e certificati**.
8. Selezionare ciascuno dei menu a discesa delle autorizzazioni (chiave, segreto, certificato), quindi **Seleziona tutto** nella parte superiore dell'elenco del menu per selezionare tutte le autorizzazioni disponibili. Dovresti avere:
   - **Autorizzazioni chiave**: 20 selezionate
   - **Autorizzazioni segrete**: 8 selezionate
   - **Autorizzazioni del certificato**: 16 selezionate

Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. Fare clic su **Avanti** per selezionare l'applicazione Azure registrata **Principale** creata inRegistrazione dell'applicazione Azure . Selezionare **Avanti**.

   È possibile assegnare un solo mandante a ogni polizza.



10. Fare clic due volte su **Avanti** fino ad arrivare a **Revisiona e crea**. Quindi, fai clic su **Crea**.
11. Selezionare **Avanti** per passare alle opzioni di **Rete**.
12. Selezionare il metodo di accesso alla rete appropriato oppure selezionare **Tutte le reti** e **Revisiona + Crea** per creare il vault delle chiavi. (Il metodo di accesso alla rete può essere prescritto da una policy di governance o dal team di sicurezza cloud aziendale.)
13. Registra l'URI del Key Vault: nel Key Vault creato, vai al menu Panoramica e copia l'**URI del Vault** dalla colonna di destra. Ti servirà per un passaggio successivo.

Crea chiave di crittografia

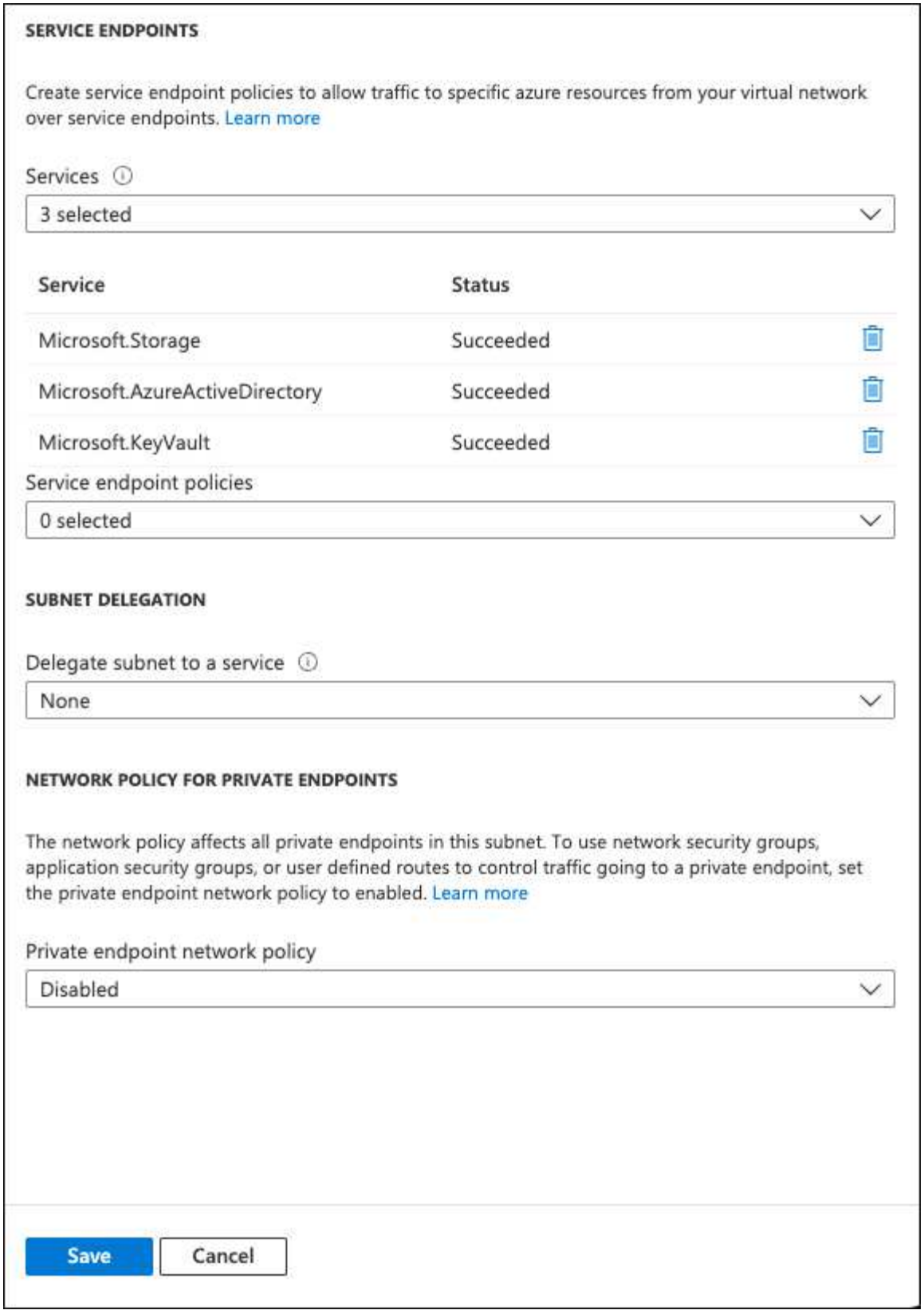
1. Nel menu del Key Vault creato per Cloud Volumes ONTAP, vai all'opzione **Chiavi**.
2. Selezionare **Genera/importa** per creare una nuova chiave.
3. Lasciare l'opzione predefinita impostata su **Genera**.
4. Fornire le seguenti informazioni:
   - Nome della chiave di crittografia

- Tipo di chiave: RSA
- Dimensione chiave RSA: 2048
- Abilitato: Sì

5. Selezionare **Crea** per creare la chiave di crittografia.
6. Torna al menu **Chiavi** e seleziona la chiave appena creata.
7. Selezionare l'ID chiave in **Versione corrente** per visualizzare le proprietà della chiave.
8. Individuare il campo **Identificatore chiave**. Copia l'URI fino alla stringa esadecimale esclusa.

Creare un endpoint di Azure Active Directory (solo HA)

1. Questo processo è necessario solo se si sta configurando Azure Key Vault per un sistema HA Cloud Volumes ONTAP .
2. Nel portale di Azure, passare a **Reti virtuali**.
3. Selezionare la rete virtuale in cui è stato distribuito il sistema Cloud Volumes ONTAP e selezionare il menu **Sottoreti** sul lato sinistro della pagina.
4. Seleziona dall'elenco il nome della subnet per la distribuzione Cloud Volumes ONTAP .
5. Passare all'intestazione **Endpoint di servizio**. Nel menu a discesa, seleziona quanto segue:
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage** (facoltativo)



6. Seleziona **Salva** per acquisire le tue impostazioni.

Configurazione Cloud Volumes ONTAP

1. Connettiti al LIF di gestione del cluster con il tuo client SSH preferito.
2. Accedi alla modalità privilegio avanzata in ONTAP:

```
set advanced -con off
```

3. Identificare l'SVM dati desiderato e verificarne la configurazione DNS:
   `vserver services name-service dns show`

   a. Se esiste una voce DNS per l'SVM dati desiderato e contiene una voce per il DNS di Azure, non è richiesta alcuna azione. In caso contrario, aggiungere una voce del server DNS per l'SVM dati che punti al DNS di Azure, al DNS privato o al server locale. Dovrebbe corrispondere alla voce per l'SVM di amministrazione del cluster:
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. Verificare che il servizio DNS sia stato creato per i dati SVM:
   `vserver services name-service dns show`

4. Abilita Azure Key Vault utilizzando l'ID client e l'ID tenant salvati dopo la registrazione dell'applicazione:
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > IL `_full_key_URI` il valore deve utilizzare il `<https:// <key vault host name>/keys/<key label>` formato.

5. Dopo aver abilitato correttamente Azure Key Vault, immettere `client secret value` quando richiesto.

6. Controllare lo stato del gestore delle chiavi:
   `security key-manager external azure check` L'output sarà simile al seguente:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

Se il `service_reachability` lo stato non è `OK` , l'SVM non riesce a raggiungere il servizio Azure Key Vault con tutta la connettività e le autorizzazioni richieste. Assicurati che i criteri di rete e il routing di Azure non impediscano alla tua rete virtuale privata di raggiungere l'endpoint pubblico di Azure Key Vault. In tal caso, valutare l'utilizzo di un endpoint privato di Azure per accedere al Key Vault dall'interno della rete virtuale. Potrebbe anche essere necessario aggiungere una voce host statica sulla SVM per risolvere

l'indirizzo IP privato per l'endpoint.

IL `kms_wrapped_key_status` riferirà `UNKNOWN` nella configurazione iniziale. Il suo stato cambierà in `OK` dopo che il primo volume è stato crittografato.

7. FACOLTATIVO: creare un volume di prova per verificare la funzionalità di NVE.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   Se configurato correttamente, Cloud Volumes ONTAP creerà automaticamente il volume e abiliterà la crittografia del volume.

8. Verificare che il volume sia stato creato e crittografato correttamente. Se lo è, il `-is-encrypted` il parametro verrà visualizzato come `true` .
   `vol show -vserver SVM_name -fields is-encrypted`
9. Facoltativo: se si desidera aggiornare le credenziali sul certificato di autenticazione di Azure Key Vault, utilizzare il comando seguente:
   `security key-manager external azure update-credentials -vserver v1 -authentication-method certificate`

Link correlati

- "Configurare Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in Azure"
- "Documentazione di Microsoft Azure: Informazioni su Azure Key Vault"
- "Guida di riferimento ai comandi ONTAP"

Gestisci le chiavi di crittografia Cloud Volumes ONTAP con Google Cloud KMS

Puoi usare"Servizio di gestione delle chiavi di Google Cloud Platform (Cloud KMS)" per proteggere le chiavi di crittografia Cloud Volumes ONTAP in un'applicazione distribuita su Google Cloud Platform.

La gestione delle chiavi con Cloud KMS può essere abilitata tramite ONTAP CLI o ONTAP REST API.

Quando si utilizza Cloud KMS, tenere presente che per impostazione predefinita viene utilizzato il LIF di un SVM di dati per comunicare con l'endpoint di gestione delle chiavi cloud. Per comunicare con i servizi di autenticazione del provider cloud (oauth2.googleapis.com) viene utilizzata una rete di gestione dei nodi. Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Prima di iniziare

- Il tuo sistema dovrebbe eseguire Cloud Volumes ONTAP 9.10.1 o versione successiva
- È necessario utilizzare una SVM dati. Cloud KMS può essere configurato solo su una SVM dati.
- Devi essere un amministratore del cluster o SVM
- La licenza Volume Encryption (VE) deve essere installata sull'SVM
- A partire da Cloud Volumes ONTAP 9.12.1 GA, è necessario installare anche la licenza MTEKM (Multi-tenant Encryption Key Management)
- È richiesto un abbonamento attivo a Google Cloud Platform

Configurazione

Google Cloud

1. Nel tuo ambiente Google Cloud,"creare un portachiavi GCP simmetrico e una chiave" .
2. Assegna un ruolo personalizzato alla chiave Cloud KMS e all'account di servizio Cloud Volumes ONTAP .
   a. Crea il ruolo personalizzato:

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

   b. Assegna il ruolo personalizzato che hai creato:
   `gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`

> Se utilizzi Cloud Volumes ONTAP 9.13.0 o versione successiva, non è necessario creare un ruolo personalizzato. È possibile assegnare il predefinito[`cloudkms.cryptoKeyEncrypterDecrypter` ^] ruolo.

3. Scarica la chiave JSON dell'account di servizio:
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Connettiti al LIF di gestione del cluster con il tuo client SSH preferito.
2. Passa al livello di privilegio avanzato:
   `set -privilege advanced`
3. Creare un DNS per i dati SVM.
   `dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*
4. Crea voce CMEK:
   `security key-manager external gcp enable -vserver` *`SVM_name`* `-project-id` *`project`* `-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
5. Quando richiesto, inserisci la chiave JSON dell'account di servizio dal tuo account GCP.
6. Conferma che il processo abilitato è riuscito:

`security key-manager external gcp check -vserver svm_name`

7. FACOLTATIVO: creare un volume per testare la crittografia `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Risoluzione dei problemi

Se hai bisogno di risolvere un problema, puoi seguire i log REST API non elaborati negli ultimi due passaggi sopra:

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Abilita le soluzioni di protezione ransomware NetApp per Cloud Volumes ONTAP

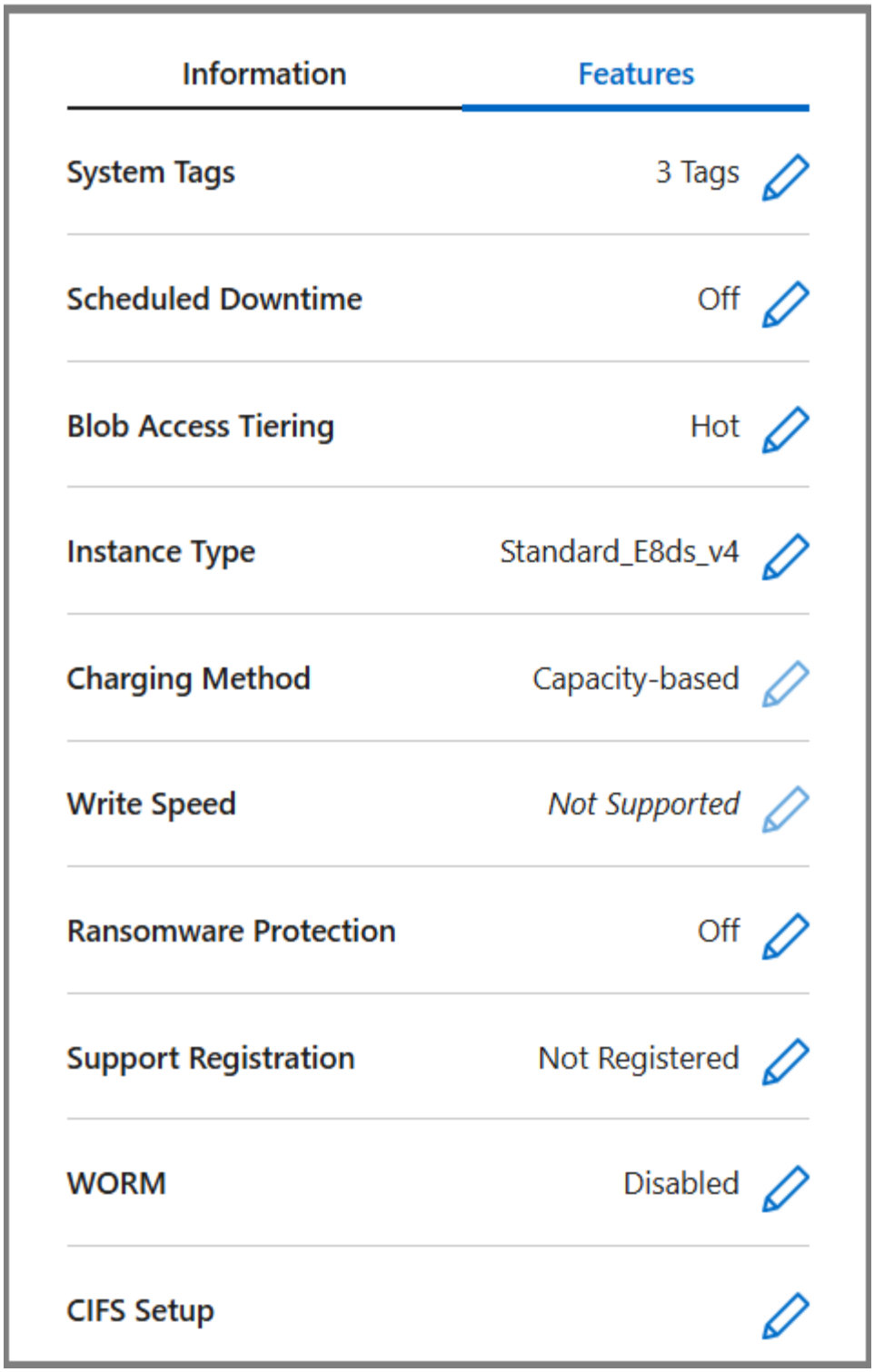
Gli attacchi ransomware possono costare alle aziende tempo, risorse e reputazione. NetApp Console consente di implementare due soluzioni NetApp contro il ransomware: protezione dalle estensioni di file ransomware più comuni e protezione autonoma dal ransomware (ARP). Queste soluzioni forniscono strumenti efficaci per la visibilità, il rilevamento e la correzione.

Protezione dalle estensioni di file ransomware più comuni

Disponibile sulla Console, l'impostazione Protezione ransomware consente di utilizzare la funzionalità ONTAP FPolicy per proteggersi dai comuni tipi di estensione di file ransomware.

Passi

1. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema Cloud Volumes ONTAP configurato per utilizzare la protezione ransomware.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Protezione ransomware**.



3. Implementare la soluzione NetApp contro il ransomware:

   a. Fare clic su **Attiva criterio snapshot** se si dispone di volumi per i quali non è abilitato un criterio snapshot.

      La tecnologia NetApp Snapshot offre la migliore soluzione del settore per la remediation del ransomware. La chiave per un ripristino riuscito è il ripristino da backup non infetti. Le copie snapshot sono di sola lettura, il che impedisce la corruzione da parte del ransomware. Possono anche fornire la granularità necessaria per creare immagini di una singola copia di file o una soluzione completa di disaster recovery.

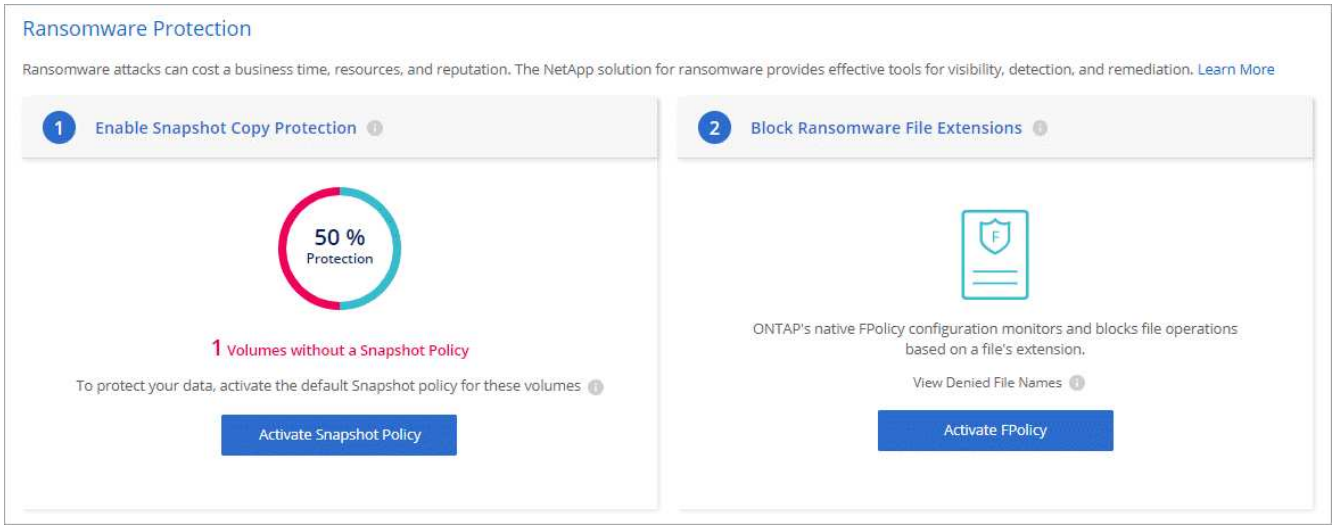
b. Fare clic su **Attiva FPolicy** per abilitare la soluzione FPolicy di ONTAP, che può bloccare le operazioni sui file in base all'estensione del file.

   Questa soluzione preventiva migliora la protezione dagli attacchi ransomware bloccando i tipi di file ransomware più comuni.

   L'ambito FPolicy predefinito blocca i file con le seguenti estensioni:

   micro, crittografato, bloccato, crittografato, criptato, critto, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, buono, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

   Questo ambito viene creato quando si attiva FPolicy su Cloud Volumes ONTAP. L'elenco si basa sui tipi di file ransomware più comuni. È possibile personalizzare le estensioni dei file bloccati utilizzando i comandi *vserver fpolicy policy scope* dalla CLI di Cloud Volumes ONTAP .



Protezione autonoma dal ransomware

Cloud Volumes ONTAP supporta la funzionalità Autonomous Ransomware Protection (ARP), che esegue analisi sui carichi di lavoro per rilevare in modo proattivo e avvisare in caso di attività anomale che potrebbero indicare un attacco ransomware.

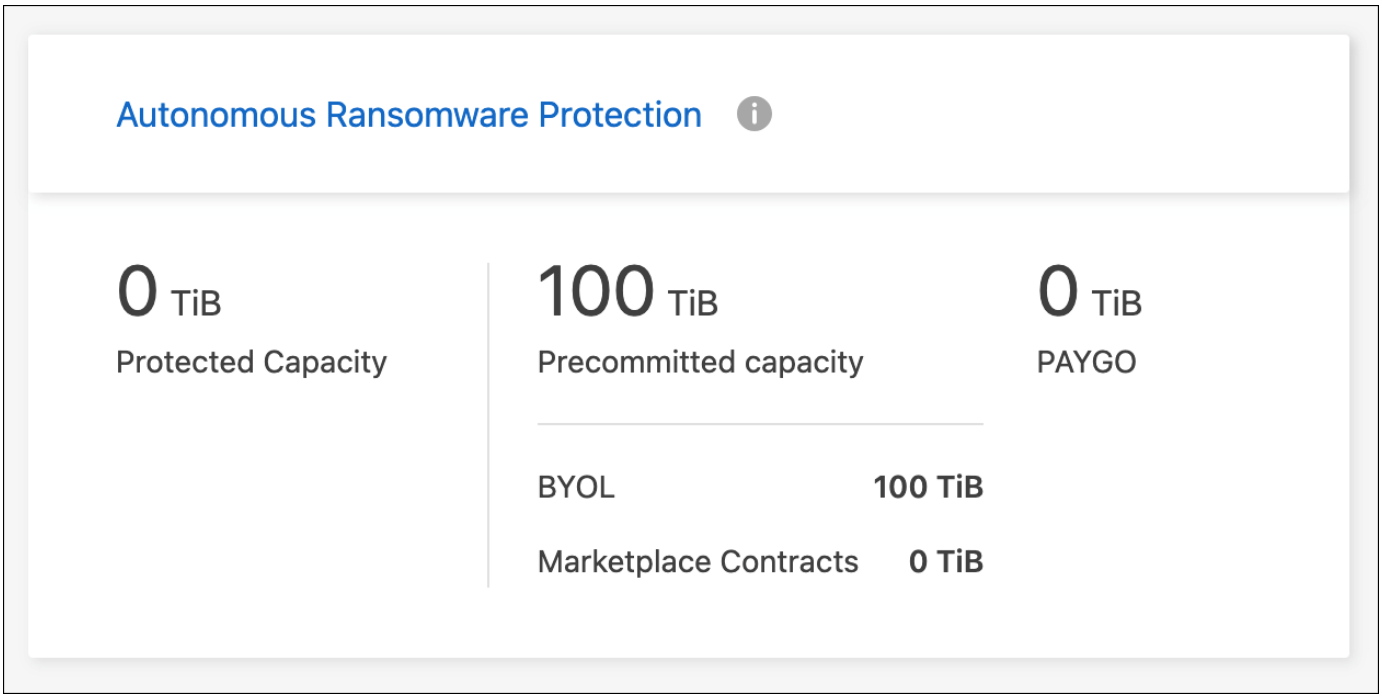
Separato dalle protezioni delle estensioni dei file fornite tramite "impostazione di protezione ransomware" , la funzionalità ARP utilizza l'analisi del carico di lavoro per avvisare l'utente di potenziali attacchi in base alle "attività anomale" rilevate. Per una protezione ransomware completa è possibile utilizzare insieme sia l'impostazione di protezione ransomware sia la funzionalità ARP.

La funzionalità ARP è disponibile per l'uso con la licenza BYOL (Bring Your Own License) e gli abbonamenti Marketplace per le tue licenze senza costi aggiuntivi.

I volumi abilitati per ARP hanno uno stato designato di "Modalità di apprendimento" o "Attivo".

La configurazione di ARP per i volumi viene eseguita tramite ONTAP System Manager e ONTAP CLI.

Per ulteriori informazioni su come abilitare ARP con ONTAP System Manager e ONTAP CLI, fare riferimento a "Documentazione ONTAP : Abilita la protezione autonoma dal ransomware" .



Crea copie Snapshot a prova di manomissione dei file WORM su Cloud Volumes ONTAP

È possibile creare copie Snapshot a prova di manomissione di file WORM (write once, read many) su un sistema Cloud Volumes ONTAP e conservare gli snapshot in forma non modificata per un periodo di conservazione specifico. Questa funzionalità è basata sulla tecnologia SnapLock e fornisce un ulteriore livello di protezione e conformità dei dati.

Prima di iniziare

Assicurarsi che il volume utilizzato per creare copie Snapshot sia un volume SnapLock . Per informazioni sull'abilitazione della protezione SnapLock sui volumi, fare riferimento a "Documentazione ONTAP : Configurare SnapLock" .

Passi

1. Crea copie Snapshot dal volume SnapLock . Per informazioni sulla creazione di copie Snapshot tramite CLI o System Manager, fare riferimento a "Documentazione ONTAP : Panoramica sulla gestione delle copie Snapshot locali" .

   Le copie Snapshot ereditano le proprietà WORM del volume, rendendole a prova di manomissione. La tecnologia SnapLock di base garantisce che uno snapshot rimanga protetto da modifiche ed eliminazioni fino alla scadenza del periodo di conservazione specificato.

2. È possibile modificare il periodo di conservazione se è necessario modificare questi snapshot. Per informazioni fare riferimento al "Documentazione ONTAP : Imposta il tempo di conservazione" .

> Anche se una copia Snapshot è protetta per un periodo di conservazione specifico, il volume di origine può essere eliminato da un amministratore del cluster, poiché l'archiviazione WORM in Cloud Volumes ONTAP funziona secondo un modello di "amministratore di archiviazione attendibile". Inoltre, un amministratore cloud fidato può eliminare i dati WORM agendo sulle risorse di archiviazione cloud.

Link correlati

- Per ulteriori informazioni su WORM, fare riferimento a"Scopri di più sullo storage WORM su Cloud Volumes ONTAP" .
- Per informazioni sulla ricarica dei volumi SnapLock , fare riferimento a"Licenze e addebiti in Cloud Volumes ONTAP" .

Amministrazione di sistema

Aggiorna Cloud Volumes ONTAP

Aggiorna Cloud Volumes ONTAP dalla NetApp Console per accedere alle ultime novità e ai miglioramenti. È necessario preparare i sistemi Cloud Volumes ONTAP prima di aggiornare il software.

Panoramica dell'aggiornamento

Prima di avviare il processo di aggiornamento Cloud Volumes ONTAP , è necessario tenere presente quanto segue.

Aggiorna solo dalla console

Non dovresti aggiornare Cloud Volumes ONTAP tramite ONTAP System Manager o ONTAP CLI, ma solo tramite la Console. In caso contrario, la stabilità del sistema potrebbe risentirne.

La console offre due modi per aggiornare Cloud Volumes ONTAP:

- Seguendo le notifiche di aggiornamento che appaiono sul sistema
- Posizionando l'immagine di aggiornamento in una posizione HTTPS e quindi fornendo alla Console l'URL

Percorsi di aggiornamento supportati

La versione di Cloud Volumes ONTAP a cui è possibile effettuare l'aggiornamento dipende dalla versione attualmente in esecuzione. Ogni versione generica o patch in una release nelle tabelle seguenti rappresenta la versione base disponibile per l'aggiornamento. Per dettagli sulle patch disponibili, fare riferimento a "note di rilascio versionate" per ciascuna release.

Percorsi di aggiornamento supportati per AWS

Versione attuale	Versioni a cui puoi effettuare l'aggiornamento diretto
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1

Versione attuale	Versioni a cui puoi effettuare l'aggiornamento diretto
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9,8	9.9.1
9,7	9,8
9,6	9,7
9,5	9,6
9,4	9,5
9,3	9,4
9,2	9,3
9,1	9,2
9,0	9,1
8,3	9,0

Percorsi di aggiornamento supportati per Azure

Versione attuale	Versioni a cui puoi effettuare l'aggiornamento diretto
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10

Versione attuale	Versioni a cui puoi effettuare l'aggiornamento diretto
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

Se disponi di una versione precedente di Cloud Volumes ONTAP in Azure, devi prima eseguire l'aggiornamento alla versione successiva e seguire i percorsi di aggiornamento supportati per raggiungere la versione di destinazione. Ad esempio, se si dispone di Cloud Volumes ONTAP 9.7 P7, seguire questo percorso di aggiornamento:

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15
- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Percorsi di aggiornamento supportati per Google Cloud

Versione attuale	Versioni a cui puoi effettuare l'aggiornamento diretto
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1

Versione attuale	Versioni a cui puoi effettuare l'aggiornamento diretto
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9,8	9.9.1
9,7	9,8
9,6	9,7
9,5	9,6
9,4	9,5
9,3	9,4
9,2	9,3
9,1	9,2
9,0	9,1
8,3	9,0

Notare quanto segue:

- I percorsi di aggiornamento supportati per Cloud Volumes ONTAP sono diversi da quelli per un cluster ONTAP locale.
- Se esegui l'aggiornamento seguendo le notifiche visualizzate in un sistema, la Console ti chiederà di eseguire l'aggiornamento a una versione che segue questi percorsi di aggiornamento supportati.
- Se esegui l'aggiornamento posizionando un'immagine di aggiornamento in una posizione HTTPS, assicurati di seguire questi percorsi di aggiornamento supportati.
- In alcuni casi, potrebbe essere necessario effettuare più aggiornamenti per raggiungere la versione desiderata.

  Ad esempio, se stai utilizzando la versione 9.8 e vuoi eseguire l'aggiornamento alla versione 9.10.1, devi prima eseguire l'aggiornamento alla versione 9.9.1 e poi alla 9.10.1.

Rilasci di patch

A partire da gennaio 2024, gli aggiornamenti delle patch saranno disponibili solo se sarà disponibile una patch per le tre versioni più recenti di Cloud Volumes ONTAP. Occasionalmente sono disponibili versioni patch per la distribuzione, quando la versione RC o GA non è disponibile per la distribuzione.

Utilizziamo l'ultima versione GA per determinare le tre versioni più recenti da visualizzare nella Console. Ad esempio, se la versione GA corrente è 9.13.1, nella Console vengono visualizzate le patch per 9.11.1-9.13.1.

Per le versioni di patch 9.11.1 o precedenti, sarà necessario utilizzare una procedura di aggiornamento manuale tramitescaricando l'immagine ONTAP .

Come regola generale per le versioni di patch, è possibile eseguire l'aggiornamento da una versione di patch inferiore a qualsiasi versione di patch superiore nella stessa versione o in quella successiva Cloud Volumes ONTAP .

Ecco un paio di esempi:

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

Ripristino o declassamento

Il ripristino o il downgrade Cloud Volumes ONTAP a una versione precedente non è supportato.

Registrazione del supporto

Per poter aggiornare il software utilizzando uno dei metodi descritti in questa pagina, è necessario registrare Cloud Volumes ONTAP presso il supporto NetApp . Ciò vale sia per il sistema pay-as-you-go (PAYGO) sia per quello bring your own license (BYOL). Avrai bisogno di"registrare manualmente i sistemi PAYGO" , mentre i sistemi BYOL sono registrati per impostazione predefinita.

Un sistema non registrato per il supporto riceverà comunque le notifiche di aggiornamento software che appaiono nella Console quando è disponibile una nuova versione. Ma prima di poter aggiornare il software sarà necessario registrare il sistema.

Aggiornamenti del mediatore HA

La console aggiorna anche l'istanza del mediatore secondo necessità durante il processo di aggiornamento Cloud Volumes ONTAP .

Aggiornamenti in AWS con tipi di istanza EC2 c4, m4 e r4

Cloud Volumes ONTAP non supporta più i tipi di istanza EC2 c4, m4 e r4. È possibile aggiornare le distribuzioni esistenti alle versioni 9.8-9.12.1 Cloud Volumes ONTAP con questi tipi di istanza. Prima di effettuare l'aggiornamento ti consigliamo dicambiare il tipo di istanza . Se non è possibile modificare il tipo di istanza, è necessarioabilitare una rete avanzata prima di effettuare l'aggiornamento. Per saperne di più sulla modifica del tipo di istanza e sull'abilitazione della rete avanzata, leggere le sezioni seguenti.

In Cloud Volumes ONTAP con versione 9.13.0 e successive, non è possibile eseguire l'aggiornamento con i tipi di istanza EC2 c4, m4 e r4. In questo caso, è necessario ridurre il numero di dischi e quindicambiare il tipo di istanza oppure distribuire una nuova configurazione HA-pair con i tipi di istanza EC2 c5, m5 e r5 ed eseguire la migrazione dei dati.

Cambia il tipo di istanza

I tipi di istanza EC2 c4, m4 e r4 consentono più dischi per nodo rispetto ai tipi di istanza EC2 c5, m5 e r5. Se il numero di dischi per nodo per l'istanza EC2 c4, m4 o r4 in esecuzione è inferiore al limite massimo di spazio su disco per nodo per le istanze c5, m5 e r5, è possibile modificare il tipo di istanza EC2 in c5, m5 o r5.

"Controlla i limiti del disco e del tiering per istanza EC2" "Modifica il tipo di istanza EC2 per Cloud Volumes ONTAP"

Se non è possibile modificare il tipo di istanza, seguire i passaggi inAbilitare una rete avanzata .

Abilitare una rete avanzata

Per eseguire l'aggiornamento a Cloud Volumes ONTAP versione 9.8 e successive, è necessario abilitare la *rete avanzata* sul cluster che esegue il tipo di istanza c4, m4 o r4. Per abilitare ENA, fare riferimento all'articolo della Knowledge Base"Come abilitare reti avanzate come SR-IOV o ENA sulle istanze AWS Cloud Volumes

ONTAP" .

Preparati all'aggiornamento

Prima di eseguire un aggiornamento, è necessario verificare che i sistemi siano pronti e apportare le modifiche di configurazione necessarie.

- Pianificare i tempi di inattività
- Verificare che la restituzione automatica sia ancora abilitata
- Sospendi i trasferimenti SnapMirror
- Verificare che gli aggregati siano online
- Verificare che tutti i LIF siano sulle porte di casa

Pianificare i tempi di inattività

Quando si aggiorna un sistema a nodo singolo, il processo di aggiornamento mette il sistema offline per un massimo di 25 minuti, durante i quali l'I/O viene interrotto.

In molti casi, l'aggiornamento di una coppia HA non comporta interruzioni e l'I/O non viene interrotto. Durante questo processo di aggiornamento non distruttivo, ogni nodo viene aggiornato in tandem per continuare a fornire I/O ai client.

I protocolli orientati alla sessione potrebbero causare effetti negativi sui client e sulle applicazioni in determinate aree durante gli aggiornamenti. Per i dettagli, fare riferimento al "Documentazione ONTAP"

Verificare che la restituzione automatica sia ancora abilitata

Il giveback automatico deve essere abilitato su una coppia Cloud Volumes ONTAP HA (questa è l'impostazione predefinita). In caso contrario, l'operazione fallirà.

"Documentazione ONTAP : Comandi per la configurazione della restituzione automatica"

Sospendi i trasferimenti SnapMirror

Se un sistema Cloud Volumes ONTAP ha relazioni SnapMirror attive, è consigliabile sospendere i trasferimenti prima di aggiornare il software Cloud Volumes ONTAP . La sospensione dei trasferimenti previene i guasti SnapMirror . È necessario sospendere i trasferimenti dal sistema di destinazione.

> Anche se NetApp Backup and Recovery utilizza un'implementazione di SnapMirror per creare file di backup (denominata SnapMirror Cloud), i backup non devono essere sospesi quando un sistema viene aggiornato.

Informazioni su questo compito

Questi passaggi descrivono come utilizzare ONTAP System Manager per la versione 9.3 e successive.

Passi

1. Accedere a System Manager dal sistema di destinazione.

   È possibile accedere a System Manager indirizzando il browser Web all'indirizzo IP del LIF di gestione del cluster. È possibile trovare l'indirizzo IP nel sistema Cloud Volumes ONTAP .

Il computer da cui si accede alla Console deve disporre di una connessione di rete a Cloud Volumes ONTAP. Ad esempio, potrebbe essere necessario accedere alla Console da un jump host presente nella rete del tuo provider cloud.

2. Fare clic su **Protezione > Relazioni**.
3. Selezionare la relazione e fare clic su **Operazioni > Sospendi**.

Verificare che gli aggregati siano online

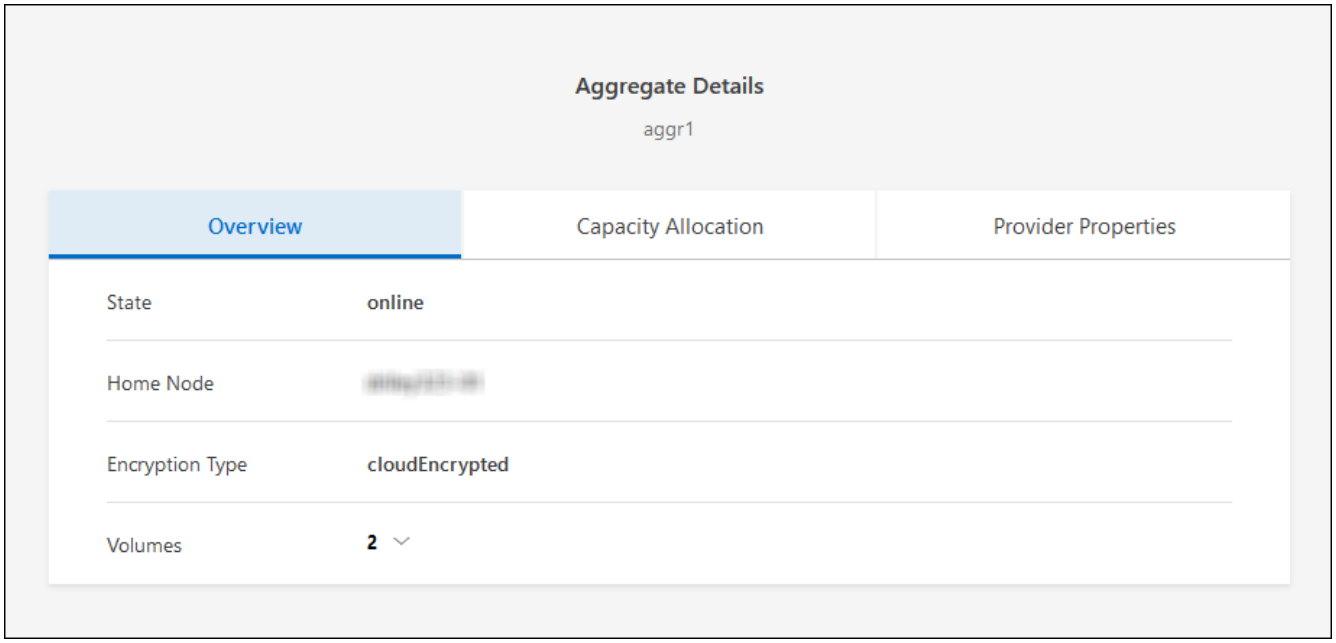
Aggregates for Cloud Volumes ONTAP deve essere online prima di aggiornare il software. Nella maggior parte delle configurazioni gli aggregati dovrebbero essere online, ma se non lo sono, è necessario attivarli.

Informazioni su questo compito

Questi passaggi descrivono come utilizzare ONTAP System Manager per la versione 9.3 e successive.

Passi

1. Nel sistema Cloud Volumes ONTAP , fare clic sulla scheda **Aggregati**.
2. Sulla tessera aggregata richiesta, fare clic su ••• icona, quindi seleziona **Visualizza dettagli aggregati**.



3. Se l'aggregato è offline, utilizzare ONTAP System Manager per riportarlo online:
   a. Fare clic su **Archiviazione > Aggregati e dischi > Aggregati**.
   b. Selezionare l'aggregato, quindi fare clic su **Altre azioni > Stato > Online**.

Verificare che tutti i LIF siano sulle porte di casa

Prima di effettuare l'aggiornamento, tutti i LIF devono trovarsi sulle porte home. Fare riferimento alla documentazione ONTAP per"verificare che tutti i LIF siano sulle porte di casa" .

Se si verifica un errore di aggiornamento, consultare l'articolo della Knowledge Base (KB)"L'aggiornamento di Cloud Volumes ONTAP non riesce" .

Aggiorna Cloud Volumes ONTAP

La Console ti avvisa quando è disponibile una nuova versione per l'aggiornamento. Da questa notifica puoi avviare il processo di aggiornamento. Per ulteriori informazioni, consultare Aggiorna dalle notifiche della console .

Un altro modo per eseguire aggiornamenti software è utilizzare un'immagine su un URL esterno. Questa opzione è utile se la console non riesce ad accedere al bucket S3 per aggiornare il software o se è stata fornita una patch. Per ulteriori informazioni, consultare Aggiorna da un'immagine disponibile a un URL .

Aggiorna dalle notifiche della console

La Console visualizza una notifica negli ambienti di lavoro Cloud Volumes ONTAP quando è disponibile una nuova versione di Cloud Volumes ONTAP :

Prima di poter aggiornare Cloud Volumes ONTAP tramite le notifiche, è necessario disporre di un account NetApp Support Site.

È possibile avviare il processo di aggiornamento da questa notifica, che automatizza il processo ottenendo l'immagine software da un bucket S3, installando l'immagine e quindi riavviando il sistema.

Prima di iniziare

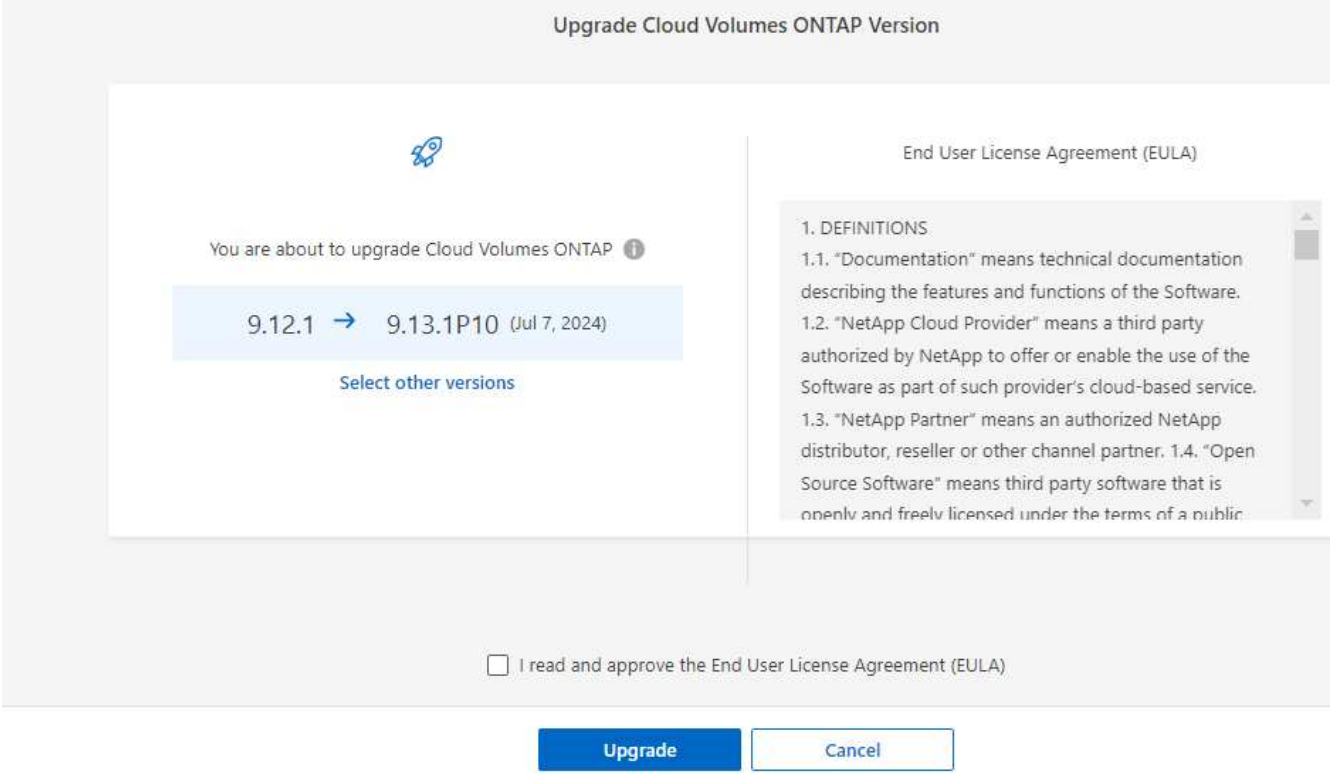
Operazioni quali la creazione di volumi o aggregati non devono essere in corso sul sistema Cloud Volumes ONTAP .

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Selezionare un sistema Cloud Volumes ONTAP .

   Se è disponibile una nuova versione, nella scheda Panoramica viene visualizzata una notifica:

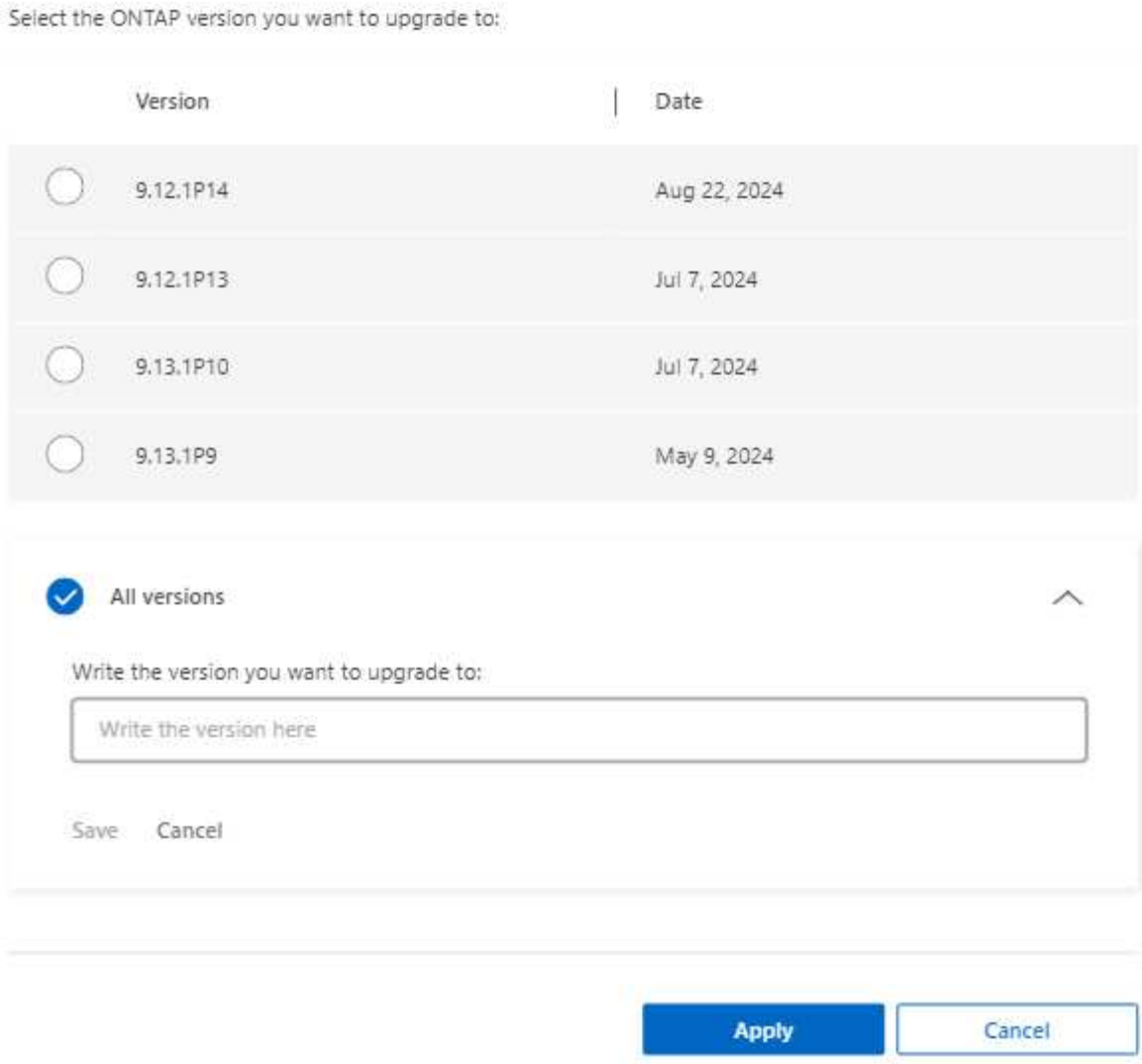
3. Se desideri aggiornare la versione installata di Cloud Volumes ONTAP, fai clic su **Aggiorna ora!** Per impostazione predefinita, viene visualizzata la versione più recente e compatibile per l'aggiornamento.



Se desideri effettuare l'aggiornamento a un'altra versione, fai clic su **Seleziona altre versioni**. Vengono elencate le ultime versioni di Cloud Volumes ONTAP compatibili anche con la versione installata sul sistema. Ad esempio, la versione installata sul tuo sistema è 9.12.1P3 e sono disponibili le seguenti versioni compatibili:

- 9.12.1P4 a 9.12.1P14
- 9.13.1 e 9.13.1P1 La versione predefinita per l'aggiornamento è 9.13.1P1, mentre le altre versioni disponibili sono 9.12.1P13, 9.13.1P14, 9.13.1 e 9.13.1P1.

4. Facoltativamente, puoi fare clic su **Tutte le versioni** per immettere un'altra versione a cui desideri effettuare l'aggiornamento (ad esempio, la patch successiva della versione installata). Per un percorso di aggiornamento compatibile della versione corrente Cloud Volumes ONTAP , fare riferimento a"Percorsi di aggiornamento supportati" .
5. Fare clic su **Salva** e poi su **Applica**



.

6. Nella pagina Upgrade Cloud Volumes ONTAP , leggere l'EULA, quindi selezionare **Ho letto e approvo l'EULA**.
7. Seleziona **Aggiorna**.
8. Per visualizzare lo stato di avanzamento, nel sistema Cloud Volumes ONTAP , selezionare **Audit**.

Risultato

La console avvia l'aggiornamento del software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sul sistema.

Dopo aver finito

Se hai sospeso i trasferimenti SnapMirror , utilizza Gestione sistema per riprenderli.

Aggiorna da un'immagine disponibile a un URL

È possibile posizionare l'immagine software Cloud Volumes ONTAP sull'agente della console o su un server HTTP e quindi avviare l'aggiornamento del software dalla console. È possibile utilizzare questa opzione se la console non riesce ad accedere al bucket S3 per aggiornare il software.

Prima di iniziare

- Operazioni quali la creazione di volumi o aggregati non devono essere in corso sul sistema Cloud Volumes

ONTAP .

- Se si utilizza HTTPS per ospitare immagini ONTAP , l'aggiornamento potrebbe non riuscire a causa di problemi di autenticazione SSL, causati da certificati mancanti. La soluzione alternativa consiste nel generare e installare un certificato firmato da una CA da utilizzare per l'autenticazione tra ONTAP e la console.

  Vai alla Knowledge Base NetApp per visualizzare le istruzioni dettagliate:

  "NetApp KB: Come configurare la console come server HTTPS per ospitare le immagini di aggiornamento"

Passi

1. Facoltativo: configurare un server HTTP in grado di ospitare l'immagine software Cloud Volumes ONTAP .

   Se si dispone di una connessione VPN alla rete virtuale, è possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP nella propria rete. Altrimenti, è necessario posizionare il file su un server HTTP nel cloud.

2. Se si utilizza un proprio gruppo di sicurezza per Cloud Volumes ONTAP, assicurarsi che le regole in uscita consentano le connessioni HTTP in modo che Cloud Volumes ONTAP possa accedere all'immagine software.

   Per impostazione predefinita, il gruppo di sicurezza Cloud Volumes ONTAP consente connessioni HTTP in uscita.

3. Ottieni l'immagine del software da "il sito di supporto NetApp" .
4. Copiare l'immagine del software in una directory sull'agente Console o su un server HTTP da cui verrà servito il file.

   Sono disponibili due percorsi. Il percorso corretto dipende dalla versione dell'agente della console.

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`

5. Nel sistema, fare clic su ••• icona, quindi fare clic su **Aggiorna Cloud Volumes ONTAP**.
6. Nella pagina Aggiorna versione Cloud Volumes ONTAP , immettere l'URL, quindi fare clic su **Modifica immagine**.

   Se hai copiato l'immagine del software nell'agente Console nel percorso indicato sopra, dovresti immettere il seguente URL:

   http://<indirizzo IP privato_agente_console>/ontap/images/<nome-file-immagine>

   Nell'URL, **nome-file-immagine** deve seguire il formato "cot.image.9.13.1P2.tgz".

7. Fare clic su **Procedi** per confermare.

Risultato

La console avvia l'aggiornamento del software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sul sistema.

Dopo aver finito

Se hai sospeso i trasferimenti SnapMirror , utilizza Gestione sistema per riprenderli.

Correggi gli errori di download quando utilizzi un gateway Google Cloud NAT

L'agente Console scarica automaticamente gli aggiornamenti software per Cloud Volumes ONTAP. Il download potrebbe non riuscire se la configurazione utilizza un gateway Google Cloud NAT. È possibile correggere questo problema limitando il numero di parti in cui è suddivisa l'immagine software. Per completare questo passaggio è necessario utilizzare le API.

Fare un passo

1. Invia una richiesta PUT a `/occm/`config con il seguente JSON come corpo:

```
{
  "maxDownloadSessions": 32
}
```

Il valore per *maxDownloadSessions* può essere 1 o qualsiasi numero intero maggiore di 1. Se il valore è 1, l'immagine scaricata non verrà divisa.

Si noti che 32 è un valore di esempio. Il valore da utilizzare dipende dalla configurazione NAT e dal numero di sessioni che è possibile avere contemporaneamente.

"Scopri di più sulla chiamata API /occm/config" .

Registra i sistemi Cloud Volumes ONTAP pay-as-you-go

Il supporto di NetApp è incluso nei sistemi Cloud Volumes ONTAP pay-as-you-go (PAYGO), ma è necessario prima attivare il supporto registrando i sistemi con NetApp.

La registrazione di un sistema PAYGO con NetApp è necessaria per aggiornare il software ONTAP utilizzando uno qualsiasi dei metodi"descritto in questa pagina" .

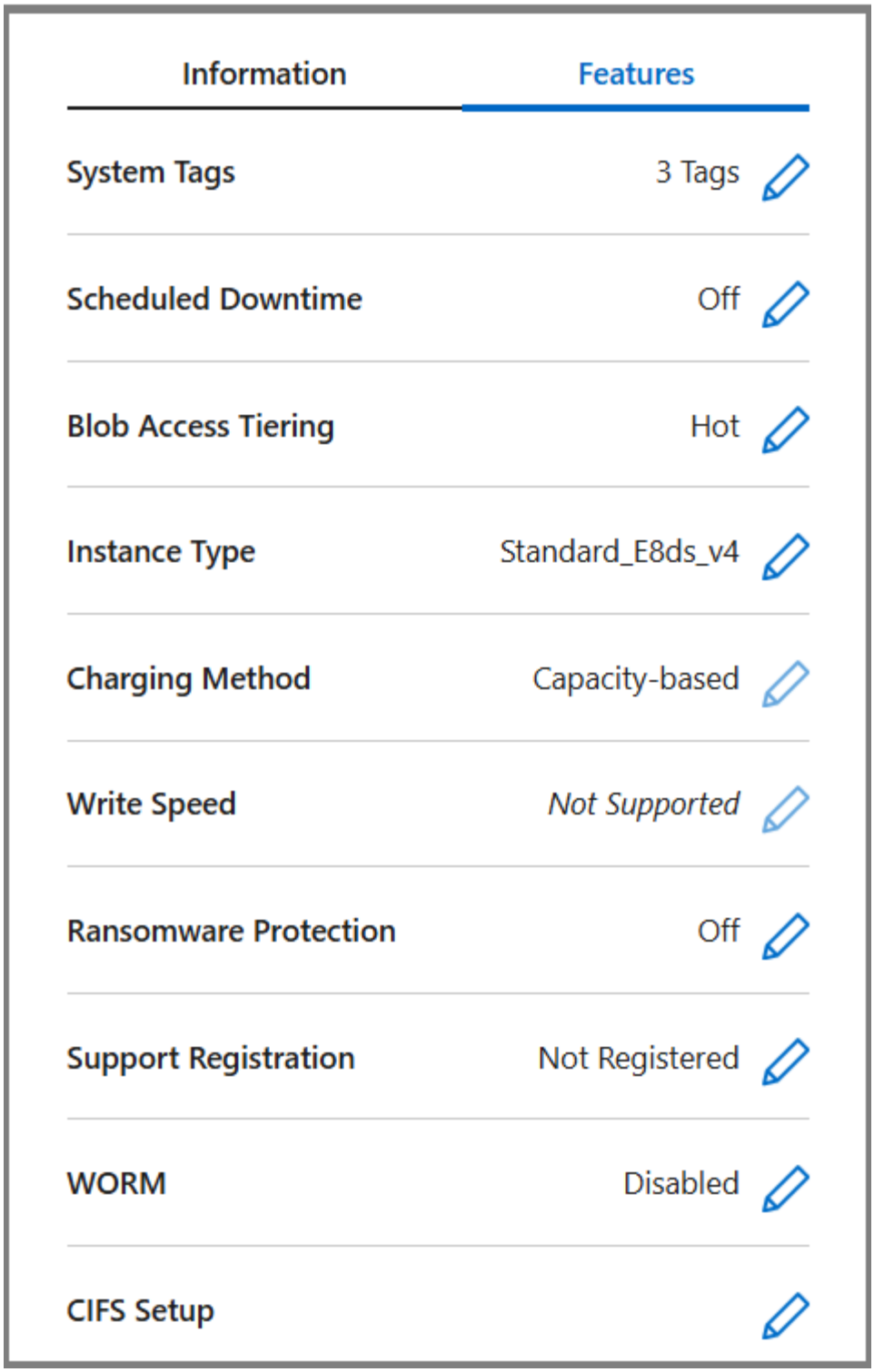
Un sistema non registrato per il supporto riceverà comunque le notifiche di aggiornamento software che compaiono nella NetApp Console quando è disponibile una nuova versione. Ma prima di poter aggiornare il software sarà necessario registrare il sistema.

Passi

1. Se non hai ancora aggiunto il tuo account NetApp Support Site alla Console, vai su **Impostazioni account** e aggiungilo ora.

   "Scopri come aggiungere account al sito di supporto NetApp" .

2. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema che si desidera registrare.
3. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Registrazione supporto**.



4. Seleziona un account del sito di supporto NetApp e fai clic su **Registrati**.

Risultato

Il sistema è registrato presso NetApp.

Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità

Dopo la fine della disponibilità (EOA) delle licenze basate sui nodi, è necessario passare

alle licenze basate sulla capacità utilizzando lo strumento di conversione delle licenze nella NetApp Console.

Per impegni annuali o a lungo termine, NetApp consiglia di contattare il proprio rappresentante NetApp prima della data EOA (11 novembre 2024) o della data di scadenza della licenza per assicurarsi che siano soddisfatti i prerequisiti per la transizione. Se non si dispone di un contratto a lungo termine per un nodo Cloud Volumes ONTAP e si esegue il sistema con un abbonamento on-demand pay-as-you-go (PAYGO), è importante pianificare la conversione prima della fine del supporto (EOS) il 31 dicembre 2024. In entrambi i casi, è necessario assicurarsi che il sistema soddisfi i requisiti prima di utilizzare lo strumento di conversione delle licenze nella NetApp Console per una transizione senza problemi.

Per informazioni su EOA ed EOS, fare riferimento a"Fine della disponibilità delle licenze basate sui nodi" .

Informazioni su questo compito

- Quando si utilizza lo strumento di conversione delle licenze, la transizione dal modello di licenza basato sui nodi a quello basato sulla capacità viene eseguita in loco e online, eliminando la necessità di qualsiasi migrazione dei dati o di provisioning di risorse cloud aggiuntive.
- Si tratta di un'operazione non dirompente, che non comporta alcuna interruzione del servizio o tempi di inattività delle applicazioni.
- I dati dell'account e delle applicazioni nel sistema Cloud Volumes ONTAP rimangono intatti.
- Le risorse cloud sottostanti rimangono inalterate dopo la conversione.
- Lo strumento di conversione delle licenze supporta tutti i tipi di distribuzione, ad esempio nodo singolo, alta disponibilità (HA) in una singola zona di disponibilità (AZ), HA in più AZ, Bring Your Own License (BYOL) e PAYGO.
- Lo strumento supporta tutte le licenze basate su nodi come origine e tutte le licenze basate su capacità come destinazione. Ad esempio, se si dispone di una licenza basata su nodi PAYGO Standard, è possibile convertirla in qualsiasi licenza basata su capacità acquistata tramite il marketplace. NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .
- La conversione è supportata da tutti i provider cloud: AWS, Azure e Google Cloud.
- Dopo la conversione, il numero di serie della licenza basata sul nodo verrà sostituito da un formato basato sulla capacità. Questa operazione viene eseguita come parte della conversione e si riflette sul tuo account NetApp Support Site (NSS).
- Quando si passa al modello basato sulla capacità, i dati continuano a essere conservati nella stessa posizione della licenza basata sui nodi. Questo approccio garantisce che non vi siano interruzioni nel posizionamento dei dati e sostiene i principi di sovranità dei dati durante tutta la transizione.

Prima di iniziare

- Dovresti avere un account NSS con accesso cliente o amministratore.
- Il tuo account NSS deve essere registrato con le credenziali utente utilizzate per accedere alla Console.
- Il sistema Cloud Volumes ONTAP deve essere collegato all'account NSS con accesso cliente o amministratore.
- È necessario disporre di una licenza valida basata sulla capacità, ovvero una licenza BYOL o un abbonamento al marketplace.
- Nel tuo account dovrebbe essere disponibile una licenza basata sulla capacità. Questa licenza può essere un abbonamento al marketplace o un pacchetto di offerte BYOL/private disponibile in * Licenses and subscriptions* nella Console.
- Prima di selezionare un pacchetto di destinazione, è necessario comprendere i seguenti criteri:

- Se l’account dispone di una licenza BYOL basata sulla capacità, il pacchetto di destinazione selezionato deve essere allineato alle licenze BYOL basate sulla capacità dell’account:
  - Quando `Professional` è selezionato come pacchetto di destinazione, l’account deve avere una licenza BYOL con un pacchetto Professional:
  - Quando `Essentials` è selezionato come pacchetto di destinazione, l’account deve avere una licenza BYOL con il pacchetto Essentials.
- Se il pacchetto di destinazione non è in linea con la disponibilità della licenza BYOL dell’account, ciò implica che la licenza basata sulla capacità potrebbe non includere il pacchetto selezionato. In questo caso, l’addebito avverrà tramite l’abbonamento al marketplace.
- Se non è disponibile una licenza BYOL basata sulla capacità, ma solo un abbonamento al marketplace, è necessario assicurarsi che il pacchetto selezionato sia incluso nell’abbonamento al marketplace basato sulla capacità.
- Se la capacità nella tua licenza basata sulla capacità esistente non è sufficiente e se hai un abbonamento al marketplace per addebitare l’utilizzo della capacità aggiuntiva, ti verrà addebitata la capacità aggiuntiva tramite l’abbonamento al marketplace.
- Se la capacità nella licenza basata sulla capacità esistente non è sufficiente e non si dispone di un abbonamento al marketplace a cui addebitare l’utilizzo della capacità aggiuntiva, la conversione non può avvenire. Dovresti aggiungere un abbonamento al marketplace per addebitare la capacità aggiuntiva o estendere la capacità disponibile alla tua licenza attuale.
- Se il pacchetto di destinazione non è in linea con la disponibilità della licenza BYOL dell’account e se la capacità della licenza basata sulla capacità esistente non è sufficiente, l’addebito verrà effettuato tramite l’abbonamento al marketplace.

Se uno qualsiasi di questi requisiti non viene soddisfatto, la conversione della licenza non avviene. In casi specifici la licenza potrebbe essere convertita, ma non utilizzabile. Fare clic sull’icona delle informazioni per identificare i problemi e adottare misure correttive.

Passi

1. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema per il quale si desidera modificare il tipo di licenza.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità.
3. Seleziona l’icona della matita accanto a **Metodo di ricarica**. Se il metodo di ricarica per il tuo sistema è `Node Based` , è possibile convertirlo in una ricarica a capacità variabile.

   L’icona è disabilitata se il sistema Cloud Volumes ONTAP è già caricato in base alla capacità o se uno qualsiasi dei requisiti non è soddisfatto.

4. Nella schermata **Converti licenze basate su nodo in licenze basate su capacità**, verifica il nome del sistema e i dettagli della licenza di origine.
5. Selezionare il pacchetto di destinazione per convertire la licenza esistente:
   - Elementi essenziali. Il valore predefinito è `Essentials` .
   - Professionale
6. Se si dispone di una licenza BYOL, è possibile selezionare la casella di controllo per eliminare la licenza basata su nodo dalla Console al termine della conversione. Se la conversione è ancora in corso, selezionando questa casella di controllo la licenza non verrà rimossa dalla Console. Questa opzione non è disponibile per gli abbonamenti al marketplace.

7. Seleziona la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fai clic su **Procedi**.

Dopo aver finito

Visualizza il nuovo numero di serie della licenza e verifica le modifiche nel menu * Licenses and subscriptions* della Console.

Prezzi in diversi iperscalari

Per i dettagli sui prezzi, vai a "Sito web NetApp Console" .

Per informazioni sulle offerte private in specifici iperscalari, scrivere a:

- AWS - awspo@netapp.com
- Azzurro - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

Avviare e arrestare un sistema Cloud Volumes ONTAP

È possibile arrestare e avviare Cloud Volumes ONTAP dalla NetApp Console per gestire i costi di elaborazione cloud.

Pianificazione degli arresti automatici di Cloud Volumes ONTAP

Potrebbe essere necessario arrestare Cloud Volumes ONTAP durante intervalli di tempo specifici per ridurre i costi di elaborazione. Invece di procedere manualmente, è possibile configurare la Console in modo che arresti e riavvii automaticamente i sistemi in momenti specifici.

Informazioni su questo compito

- Quando si pianifica un arresto automatico del sistema Cloud Volumes ONTAP , la Console posticipa l'arresto se è in corso un trasferimento dati attivo.

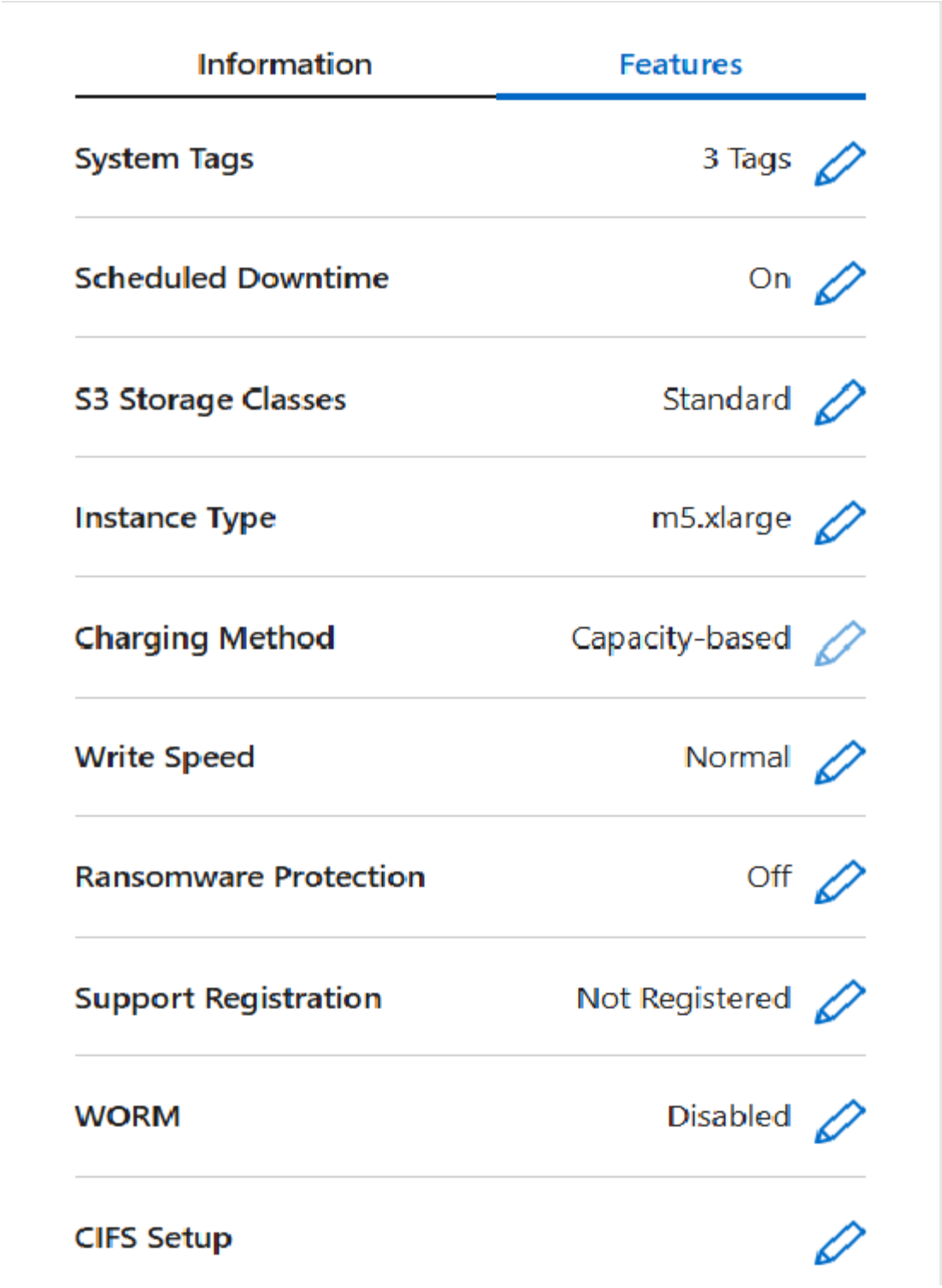
  Al termine del trasferimento, il sistema viene spento.

- Questa attività pianifica gli arresti automatici di entrambi i nodi in una coppia HA.
- Gli snapshot dei dischi di avvio e di root non vengono creati quando si disattiva Cloud Volumes ONTAP tramite arresti pianificati.

  Gli snapshot vengono creati automaticamente solo quando si esegue uno spegnimento manuale, come descritto nella sezione successiva.

Passi

1. Nella pagina **Sistemi**, fare doppio clic sul sistema Cloud Volumes ONTAP .
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Tempo di inattività pianificato**.



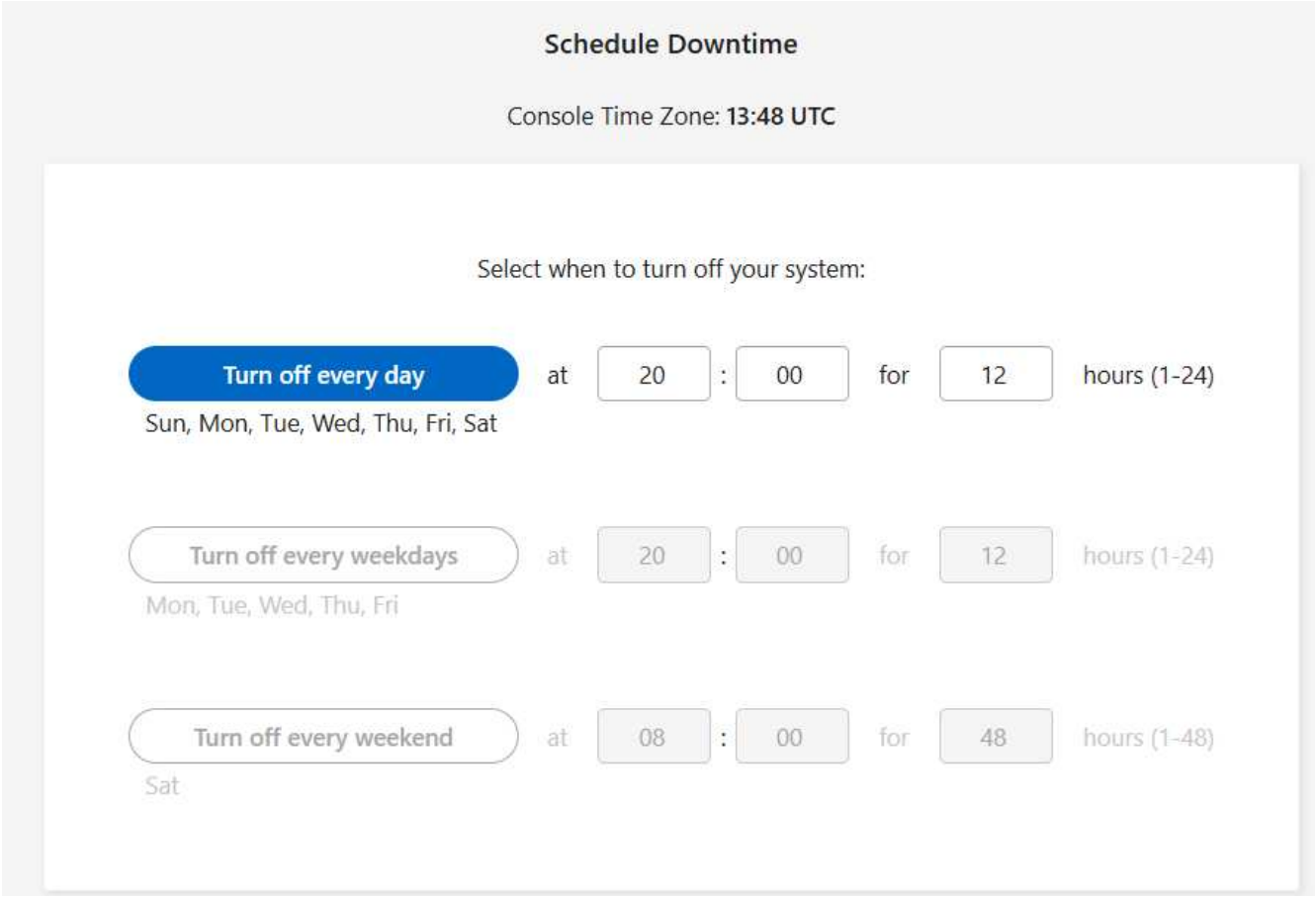
3. Specificare la pianificazione dello spegnimento:

   a. Scegli se vuoi spegnere il sistema ogni giorno, ogni giorno feriale, ogni fine settimana o una qualsiasi combinazione delle tre opzioni.

   b. Specifica quando vuoi spegnere il sistema e per quanto tempo vuoi che resti spento.

      Esempio

      L'immagine seguente mostra una pianificazione che indica alla Console di spegnere il sistema ogni sabato alle 20:00 (20:00) per 12 ore. La console riavvia il sistema ogni lunedì alle 12:00



4. Fare clic su **Salva**.

Risultato

Il programma è stato salvato. La voce corrispondente della riga Tempo di inattività programmato nel pannello Funzionalità visualizza "Attivo".

Arresto di Cloud Volumes ONTAP

L'arresto di Cloud Volumes ONTAP consente di evitare l'accumulo di costi di elaborazione e di creare snapshot dei dischi root e boot, utili per la risoluzione dei problemi.

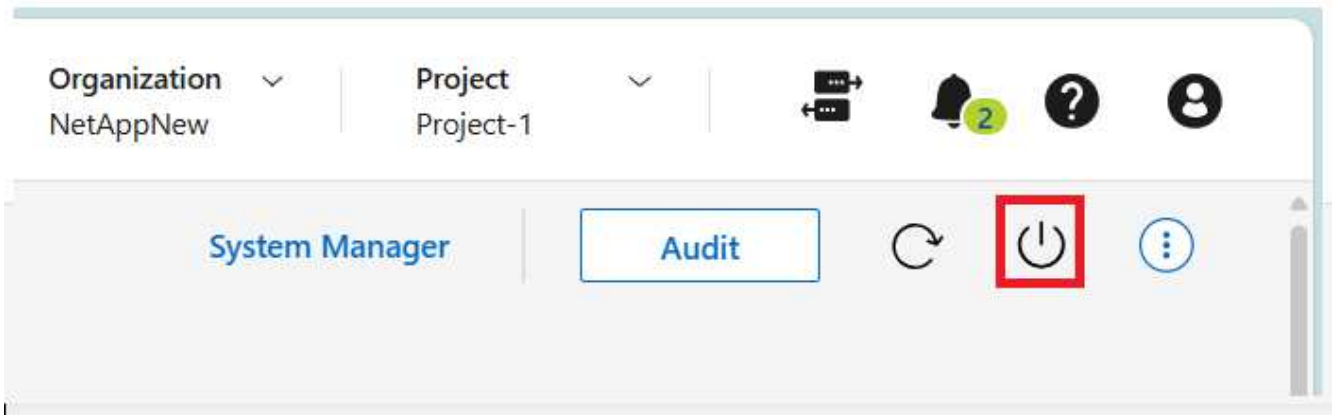
> Per ridurre i costi, la Console elimina periodicamente gli snapshot più vecchi dei dischi di root e di avvio. Vengono conservati solo i due snapshot più recenti sia per il disco di root che per quello di avvio.

Informazioni su questo compito

Quando si arresta una coppia HA, la console arresta entrambi i nodi.

Passi

1. Dal sistema, fare clic sull'icona **Disattiva**.



2. Mantenere abilitata l'opzione per creare snapshot perché gli snapshot possono abilitare il ripristino del sistema.
3. Fare clic su **Disattiva**.

   L'arresto del sistema potrebbe richiedere alcuni minuti. È possibile riavviare i sistemi in un secondo momento dalla pagina **Sistemi**.

   Gli snapshot vengono creati automaticamente al riavvio.

Sincronizza l'ora di sistema Cloud Volumes ONTAP utilizzando il server NTP

Per garantire una sincronizzazione oraria accurata, è necessario configurare un server NTP (Network Time Protocol) per i sistemi Cloud Volumes ONTAP . Assicurati di configurare un server NTP per i tuoi sistemi Cloud Volumes ONTAP su tutti i provider cloud per mantenere una sincronizzazione temporale coerente all'interno della tua rete.

Se non si configura un server NTP, potrebbero verificarsi interruzioni del servizio e una sincronizzazione oraria imprecisa.

È possibile specificare un server NTP utilizzando:

- "L'API NetApp Console".
- Il comando CLI ONTAP "creazione del server NTP del servizio orario del cluster".

Link correlati

- Articolo della Knowledge Base (KB): "In che modo un cluster CVO utilizza NTP?"
- "Preparati a utilizzare l'API"
- "Flussi di lavoro Cloud Volumes ONTAP"
- "Ottieni gli identificatori richiesti"
- "Utilizzare le API REST per NetApp Console"

Modifica la velocità di scrittura del sistema

È possibile scegliere una velocità di scrittura normale o elevata per Cloud Volumes ONTAP nella NetApp Console. La velocità di scrittura predefinita è normale. È possibile

passare a una velocità di scrittura elevata se il carico di lavoro richiede prestazioni di scrittura rapide.

L'elevata velocità di scrittura è supportata da tutti i tipi di sistemi a nodo singolo e da alcune configurazioni di coppia HA. Visualizza le configurazioni supportate in "Note sulla versione Cloud Volumes ONTAP"

Prima di modificare la velocità di scrittura, dovresti"comprendere le differenze tra le impostazioni normali e alte" .

Informazioni su questo compito

- Assicurarsi che non siano in corso operazioni quali la creazione di volumi o aggregati.
- Tieni presente che questa modifica riavvia il sistema Cloud Volumes ONTAP . Si tratta di un processo dirompente che richiede tempi di inattività per l'intero sistema.

Passi

1. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema per il quale si desidera configurare la velocità di scrittura.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Velocità di scrittura**.
3. Selezionare **Normale** o **Alto**.

   Se scegli Alto, dovrai leggere la dichiarazione "Ho capito…" e confermare selezionando la casella.

   L'opzione di velocità di scrittura **Alta** è supportata con le coppie Cloud Volumes ONTAP HA in Google Cloud a partire dalla versione 9.13.0.

4. Fare clic su **Salva**, rivedere il messaggio di conferma e quindi fare clic su **Approva**.

Modificare la password di amministrazione del cluster Cloud Volumes ONTAP

Cloud Volumes ONTAP include un account amministratore del cluster. Se necessario, puoi modificare la password per questo account dalla NetApp Console.

Non modificare la password dell'account amministratore tramite ONTAP System Manager o ONTAP CLI. La password non verrà visualizzata nella Console. Di conseguenza, la Console non riesce a monitorare correttamente l'istanza.

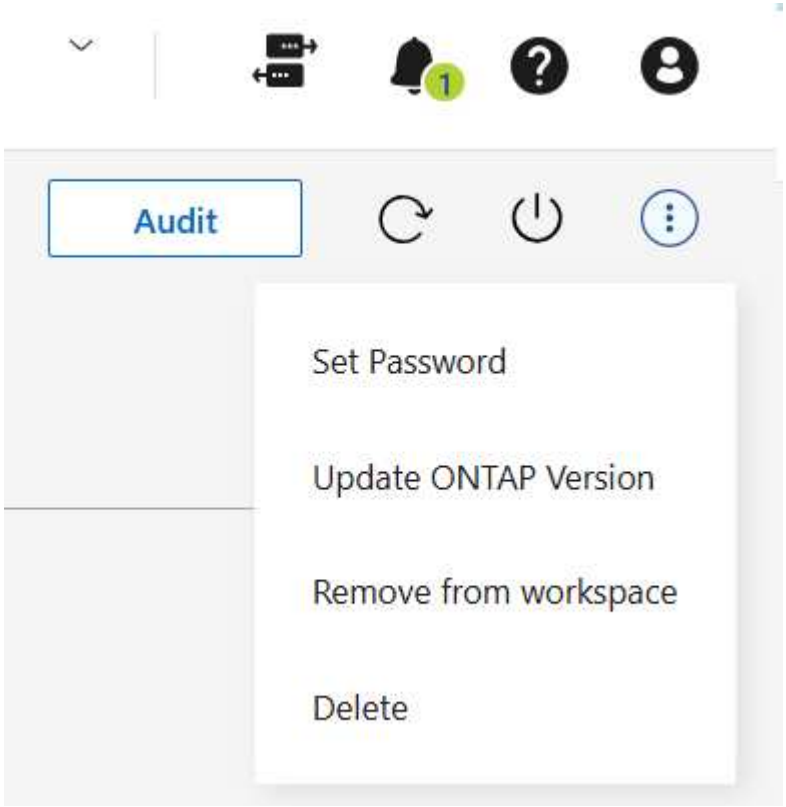
Informazioni su questo compito

La password deve rispettare alcune regole. La nuova password:

- Non dovrebbe contenere la parola `admin`
- Deve essere lungo tra otto e 50 caratteri
- Deve contenere almeno una lettera inglese e una cifra
- Non dovrebbe contenere questi caratteri speciali: `/ ( ) { } [ ] # : % " ? \`

Passi

1. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema Cloud Volumes ONTAP .
2. In alto a destra della Console, fare clic su icona e seleziona **Imposta password**.



Aggiungere, rimuovere o eliminare sistemi

Aggiungere un sistema Cloud Volumes ONTAP esistente alla NetApp Console

È possibile individuare e aggiungere i sistemi Cloud Volumes ONTAP esistenti alla NetApp Console per una gestione centralizzata. Quando si integra un sistema con un account, il sistema viene registrato con quell'account. In ambienti con più account o organizzazioni, è possibile individuare e gestire solo i sistemi registrati con il proprio account di accesso alla Console.

Quando si lavora con le registrazioni di sistema, assicurarsi che tutte le azioni vengano eseguite all'interno della stessa organizzazione e dello stesso account in cui i sistemi sono stati originariamente integrati. Ad esempio, è possibile spostare un sistema Cloud Volumes ONTAP su un nuovo agente Console quando la migrazione rimane all'interno della stessa organizzazione.

Non è possibile scoprire, visualizzare o gestire sistemi registrati con un account o un'organizzazione diversi.

Prima di iniziare

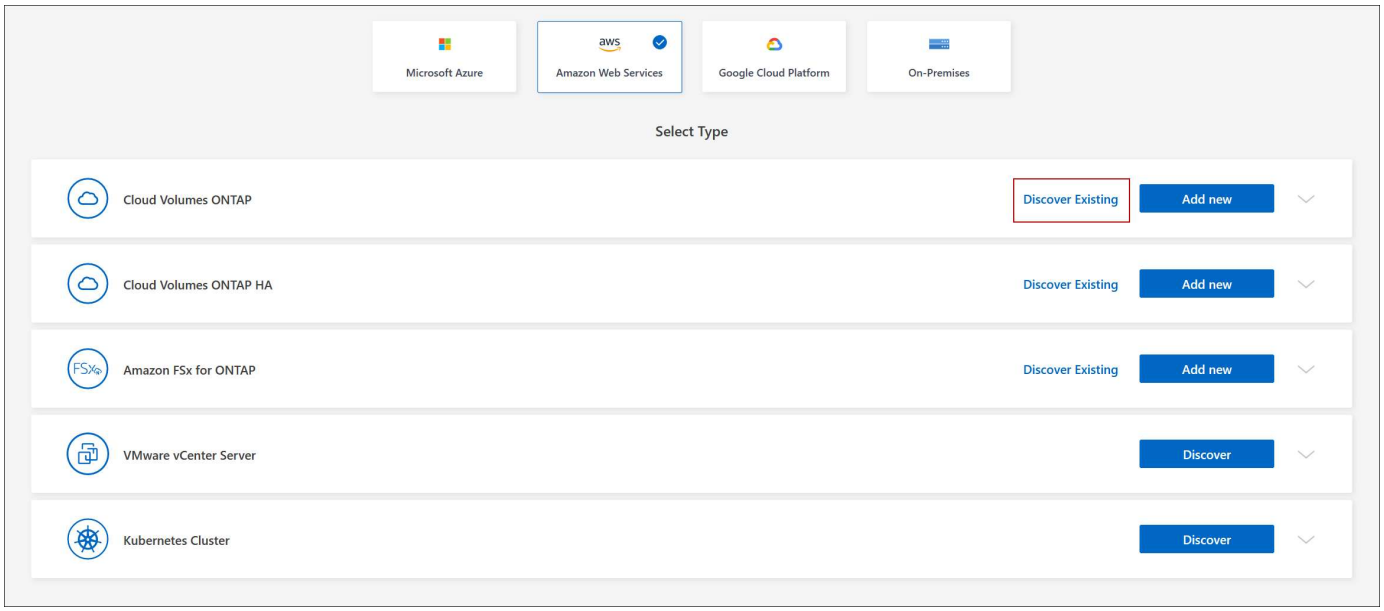
È necessario conoscere la password per l'account utente amministratore Cloud Volumes ONTAP .

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistema**, fare clic su **Aggiungi sistema**.
3. Selezionare il provider cloud in cui risiede il sistema.

4. Selezionare il tipo di sistema Cloud Volumes ONTAP da aggiungere.
5. Clicca sul link per scoprire un sistema esistente.

+



1. Nella pagina Regione, seleziona una regione. È possibile visualizzare i sistemi in esecuzione nella regione selezionata.

   In questa pagina i sistemi Cloud Volumes ONTAP sono rappresentati come istanze. Dall'elenco è possibile selezionare solo le istanze registrate con l'account corrente.

2. Nella pagina Credenziali, immettere la password per l'utente amministratore Cloud Volumes ONTAP , quindi selezionare **Vai**.

Risultato

La Console aggiunge i sistemi Cloud Volumes ONTAP alla pagina **Sistemi**.

Rimuovere un sistema Cloud Volumes ONTAP dalla NetApp Console

È possibile rimuovere un sistema Cloud Volumes ONTAP per spostarlo su un altro sistema o per risolvere problemi di individuazione.

Informazioni su questo compito

La rimozione di un sistema Cloud Volumes ONTAP lo rimuove dalla NetApp Console. Non elimina il sistema Cloud Volumes ONTAP . Se necessario, potrai riscoprire il sistema in un secondo momento.

Passi

1. Nella pagina **Sistemi**, fare doppio clic sul sistema che si desidera rimuovere.
2. In alto a destra della Console, fare clic su ••• icona e seleziona **Rimuovi dall'area di lavoro**.
3. Nella finestra **Rimuovi dall'area di lavoro**, fare clic su **Rimuovi**.

Risultato

La console rimuove il sistema. Gli utenti possono riscoprire il sistema eliminato in qualsiasi momento dalla pagina **Sistemi**.

Elimina un sistema Cloud Volumes ONTAP dalla NetApp Console

Dovresti sempre eliminare i sistemi Cloud Volumes ONTAP dalla NetApp Console, anziché dall'applicazione del tuo provider cloud. Ad esempio, se si termina un'istanza Cloud Volumes ONTAP con licenza dal proprio provider cloud, non sarà possibile utilizzare la chiave di licenza per un'altra istanza. Per rilasciare la licenza è necessario eliminare il sistema Cloud Volumes ONTAP dalla Console.

Quando si elimina un sistema, la Console termina le istanze Cloud Volumes ONTAP ed elimina dischi e snapshot.

> Altre risorse, come i backup gestiti da NetApp Backup and Recovery e le istanze per NetApp Data Classification, non vengono eliminate quando si elimina un sistema. Sarà necessario eliminarli manualmente. In caso contrario, continuerai a dover sostenere costi per queste risorse.

Quando la Console distribuisce Cloud Volumes ONTAP nel tuo provider cloud, abilita la protezione dalla terminazione sulle istanze. Questa opzione aiuta a prevenire la chiusura accidentale.

Passi

1. Se hai abilitato Backup e Ripristino sul sistema, determina se i dati sottoposti a backup sono ancora necessari e quindi "eliminare i backup, se necessario" .

   Backup e ripristino sono progettati in modo indipendente da Cloud Volumes ONTAP . Backup and Recovery non elimina automaticamente i backup quando si elimina un sistema Cloud Volumes ONTAP e attualmente nell'interfaccia utente non è presente alcun supporto per eliminare i backup dopo l'eliminazione del sistema.

2. Se hai abilitato la classificazione dei dati su questo sistema e nessun altro sistema utilizza questo servizio, devi eliminare l'istanza del servizio.

   "Scopri di più sull'istanza di classificazione dei dati" .

3. Eliminare il sistema Cloud Volumes ONTAP .
   a. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema Cloud Volumes ONTAP che si desidera eliminare.
   b. In alto a destra della Console, fare clic su ••• icona e seleziona **Elimina**.
   c. Digitare il nome del sistema che si desidera eliminare, quindi fare clic su **Elimina**. L'eliminazione di un sistema può richiedere fino a cinque minuti.

> Backup e ripristino sono gratuiti solo per le licenze Cloud Volumes ONTAP Professional. Questo vantaggio gratuito non si applica agli ambienti eliminati. Se le copie di backup dell'ambiente Cloud Volumes ONTAP vengono conservate in un'istanza di Backup and Recovery, ti verranno addebitati i costi delle copie di backup finché non verranno eliminate.

Amministrazione AWS

Modificare il tipo di istanza EC2 per un sistema Cloud Volumes ONTAP in AWS

Quando avvii Cloud Volumes ONTAP in AWS, puoi scegliere tra diverse istanze o

tipologie. Puoi modificare il tipo di istanza in qualsiasi momento se ritieni che sia troppo piccolo o troppo grande per le tue esigenze.

Informazioni su questo compito

- Il giveback automatico deve essere abilitato su una coppia Cloud Volumes ONTAP HA (questa è l'impostazione predefinita). In caso contrario, l'operazione fallirà.

  "Documentazione ONTAP 9: Comandi per la configurazione della restituzione automatica"

- La modifica del tipo di istanza può influire sui costi dei servizi AWS.
- L'operazione riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'I/O viene interrotto.

  Per le coppie HA, il cambiamento non è dirompente. Le coppie HA continuano a fornire dati.

La NetApp Console modifica un nodo alla volta avviando l'acquisizione e attendendo la restituzione. Il team di controllo qualità di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha riscontrato alcun problema sul lato client. Con la modifica delle connessioni, sono stati osservati alcuni nuovi tentativi a livello di I/O, ma il livello applicativo ha superato il ricollegamento delle connessioni NFS/CIFS.

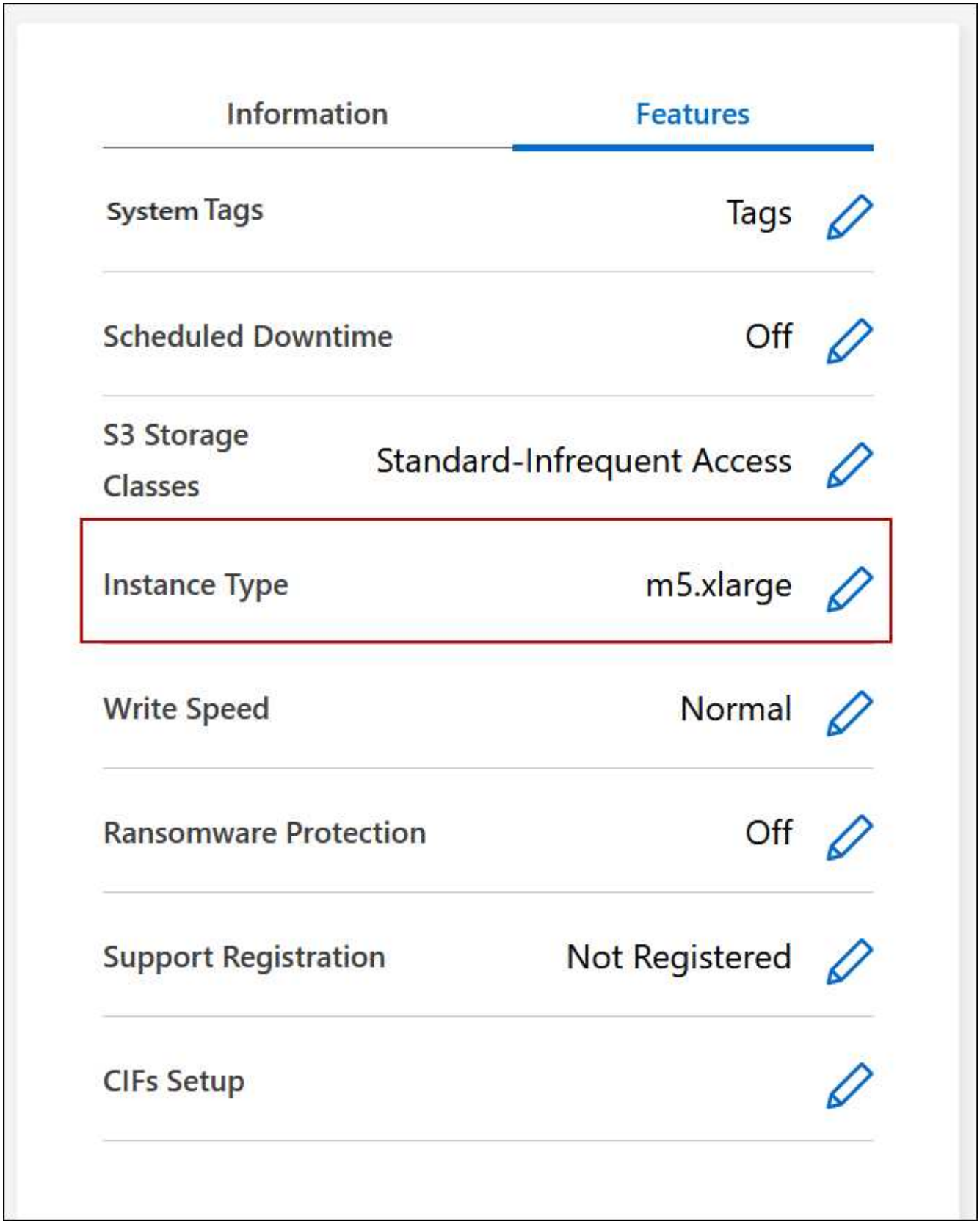
Riferimento

Per un elenco dei tipi di istanza supportati in AWS, fare riferimento a"Istanze EC2 supportate" .

Se non è possibile modificare il tipo di istanza da c4, m4 o r4, fare riferimento all'articolo della Knowledge Base"Conversione di un'istanza CVO di AWS Xen in Nitro (KVM)" .

Passi

1. Nella pagina **Sistemi**, seleziona il sistema.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Tipo di istanza**.



Se si utilizza una licenza PAYGO (Pay as you go) basata su nodi, è possibile scegliere facoltativamente una licenza e un tipo di istanza diversi facendo clic sull'icona della matita accanto a **Tipo di licenza**.

3. Scegli un tipo di istanza, seleziona la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fai clic su **Modifica**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Modificare le tabelle di routing per le coppie Cloud Volumes ONTAP HA in più zone di disponibilità AWS

È possibile modificare le tabelle di routing AWS che includono i percorsi verso gli indirizzi IP mobili per una coppia HA distribuita in più zone di disponibilità (AZ) AWS. Questa operazione può essere eseguita se nuovi client NFS o CIFS devono accedere a una coppia HA in AWS.

Passi

1. Nella pagina **Sistemi**, seleziona il sistema.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Tabelle di routing**.
3. Modificare l'elenco delle tabelle di routing selezionate e quindi fare clic su **Salva**.

Risultato

La NetApp Console invia una richiesta AWS per modificare le tabelle di routing.

Amministrazione di Azure

Modificare il tipo di VM di Azure per Cloud Volumes ONTAP

Quando avvii Cloud Volumes ONTAP in Microsoft Azure, puoi scegliere tra diversi tipi di VM. È possibile modificare il tipo di VM in qualsiasi momento se si ritiene che sia sottodimensionato o sovradimensionato per le proprie esigenze.

Informazioni su questo compito

- Il giveback automatico deve essere abilitato su una coppia Cloud Volumes ONTAP HA (questa è l'impostazione predefinita). In caso contrario, l'operazione fallirà.

  "Documentazione ONTAP 9: Comandi per la configurazione della restituzione automatica"

- La modifica del tipo di macchina virtuale può influire sui costi del servizio Microsoft Azure.
- L'operazione riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'I/O viene interrotto.

  Per le coppie HA, il cambiamento non è dirompente. Le coppie HA continuano a fornire dati.

  NetApp Console modifica un nodo alla volta avviando l'acquisizione e attendendo la restituzione. Il team di controllo qualità di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha riscontrato alcun problema sul lato client. Con la modifica delle connessioni, sono stati osservati alcuni nuovi tentativi a livello di I/O, ma il livello applicativo ha superato il ricollegamento delle connessioni NFS/CIFS.

Passi

1. Nella pagina **Sistemi**, seleziona il sistema.

2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Tipo di VM**.

   Se si utilizza una licenza PAYGO (Node-based pay-as-you-go), è possibile scegliere una licenza e un tipo di VM diversi facendo clic sull'icona della matita accanto a **Tipo di licenza**.

3. Selezionare un tipo di VM, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **Modifica**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Sostituisci i blocchi CIFS per le coppie Cloud Volumes ONTAP HA in Azure

L'amministratore dell'organizzazione o dell'account può abilitare un'impostazione nella NetApp Console che impedisce problemi con la restituzione dello storage Cloud Volumes ONTAP durante gli eventi di manutenzione di Azure. Quando si abilita questa impostazione, Cloud Volumes ONTAP pone il veto ai blocchi CIFS e reimposta le sessioni CIFS attive.

Informazioni su questo compito

Microsoft Azure pianifica periodicamente eventi di manutenzione sulle sue macchine virtuali. Quando si verifica un evento di manutenzione su una coppia Cloud Volumes ONTAP HA, la coppia HA avvia l'acquisizione dello storage. Se durante questo evento di manutenzione sono presenti sessioni CIFS attive, i blocchi sui file CIFS possono impedire la restituzione dello spazio di archiviazione.

Se si abilita questa impostazione, Cloud Volumes ONTAP porrà il veto ai blocchi e reimposterà le sessioni CIFS attive. Di conseguenza, la coppia HA può completare la restituzione dello storage durante questi eventi di manutenzione.

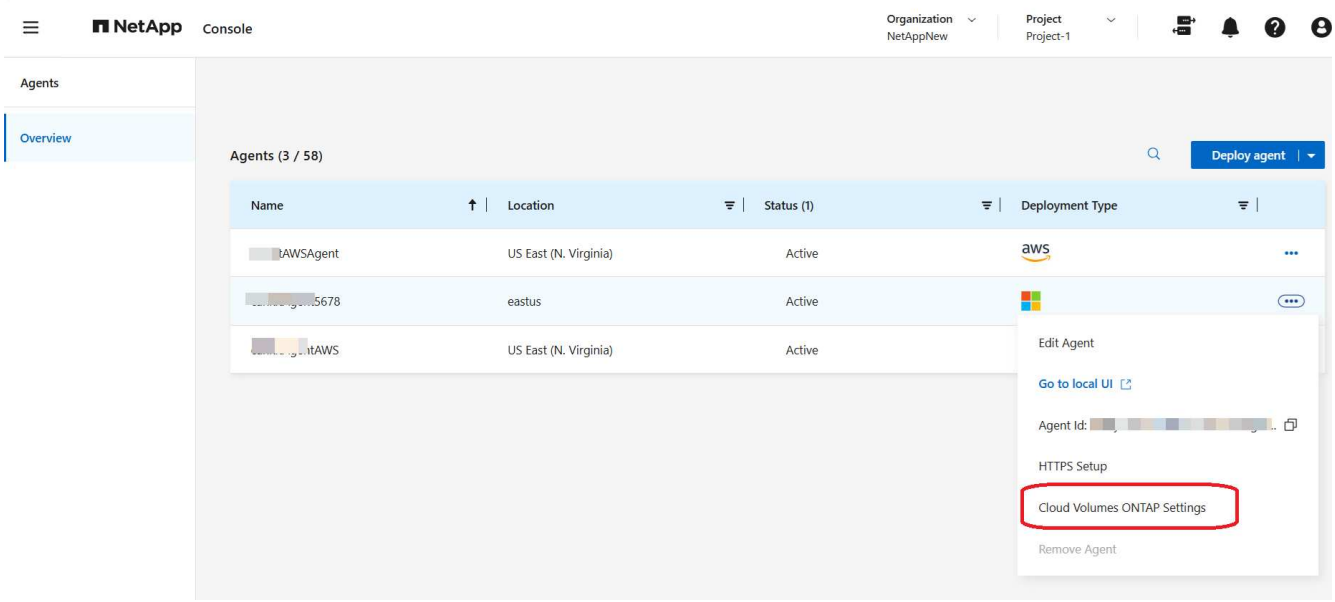
> Questo processo potrebbe risultare disfunzionale per i client CIFS. I dati non inviati dai client CIFS potrebbero andare persi.

Prima di iniziare

Prima di poter modificare le impostazioni della console, è necessario creare un agente della console. "Scopri come" .

Passi

1. Dal riquadro di navigazione a sinistra, vai su **Amministrazione > Agenti**.
2. Fare clic su ••• icona per l'agente Console che gestisce il sistema Cloud Volumes ONTAP .
3. Selezionare *Impostazioni Cloud Volumes ONTAP *.



4. In **Azure**, fare clic su **Blocchi CIFS di Azure per sistemi Azure HA**.
5. Fare clic sulla casella di controllo per abilitare la funzionalità, quindi fare clic su **Salva**.

Utilizzare un collegamento privato di Azure o endpoint di servizio per i sistemi Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza un collegamento privato di Azure per le connessioni ai relativi account di archiviazione associati. Se necessario, è possibile disabilitare i collegamenti privati di Azure e utilizzare invece gli endpoint del servizio.

Panoramica

Per impostazione predefinita, la NetApp Console abilita un collegamento privato di Azure per le connessioni tra Cloud Volumes ONTAP e i relativi account di archiviazione associati. Un collegamento privato di Azure protegge le connessioni tra gli endpoint in Azure e offre vantaggi in termini di prestazioni.

Se necessario, è possibile configurare Cloud Volumes ONTAP in modo che utilizzi endpoint di servizio anziché un collegamento privato di Azure.

Con entrambe le configurazioni, la Console limita sempre l'accesso alla rete per le connessioni tra Cloud Volumes ONTAP e gli account di archiviazione. L'accesso alla rete è limitato alla rete virtuale in cui è distribuito Cloud Volumes ONTAP e alla rete virtuale in cui è distribuito l'agente Console.

Disabilitare i collegamenti privati di Azure e utilizzare invece gli endpoint del servizio

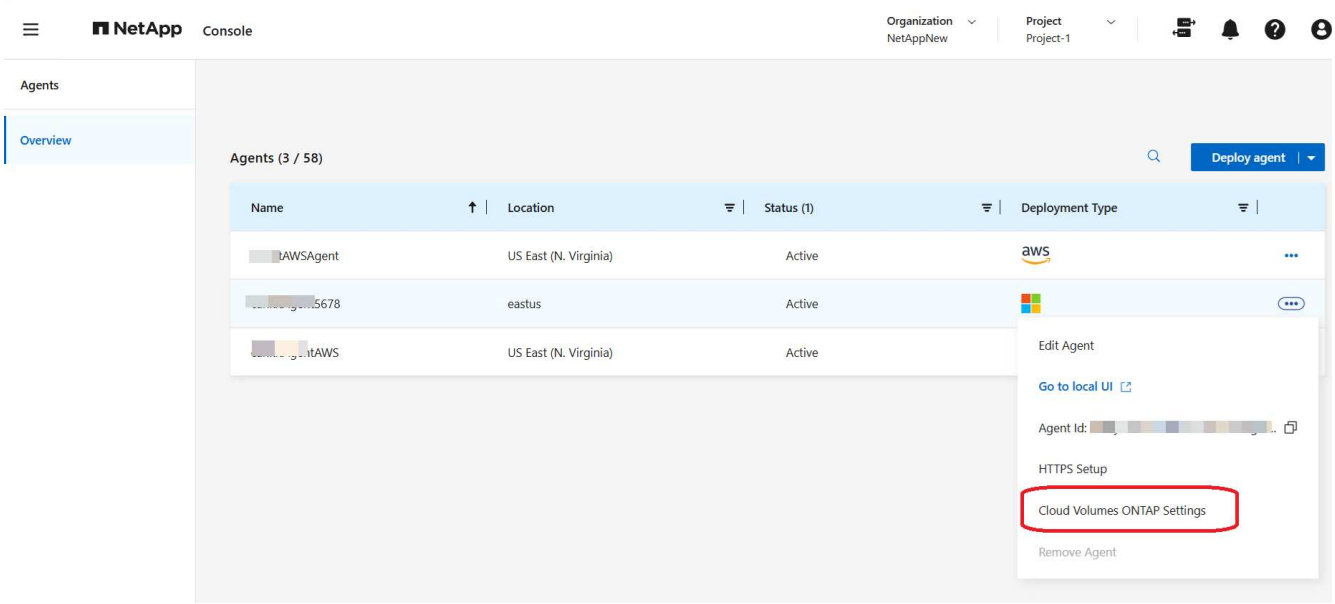
Se richiesto dalla tua azienda, puoi modificare un'impostazione nella Console in modo che Cloud Volumes ONTAP venga configurato per utilizzare endpoint di servizio anziché un collegamento privato di Azure. La modifica di questa impostazione si applica ai nuovi sistemi Cloud Volumes ONTAP creati. Gli endpoint del servizio sono supportati solo in"Coppie di regioni di Azure" tra l'agente della console e le reti virtuali Cloud Volumes ONTAP .

L'agente della console deve essere distribuito nella stessa regione di Azure dei sistemi Cloud Volumes ONTAP che gestisce oppure nella "Coppia di regioni di Azure" per i sistemi Cloud Volumes ONTAP .

Passi

1. Dal riquadro di navigazione a sinistra, vai su **Amministrazione > Agenti**.

2. Fare clic su ••• icona per l'agente Console che gestisce il sistema Cloud Volumes ONTAP .
3. Selezionare *Impostazioni Cloud Volumes ONTAP *.



4. In **Azure**, fare clic su **Usa collegamento privato di Azure**.
5. Deseleziona **Collegamento privato tra Cloud Volumes ONTAP e gli account di archiviazione**.
6. Fare clic su **Salva**.

Dopo aver finito

Se hai disabilitato i collegamenti privati di Azure e l'agente della console utilizza un server proxy, devi abilitare il traffico API diretto.

"Scopri come abilitare il traffico API diretto sull'agente Console"

Lavorare con i collegamenti privati di Azure

Nella maggior parte dei casi, non è necessario fare nulla per configurare i collegamenti privati di Azure con Cloud Volumes ONTAP. La console gestisce per te i collegamenti privati di Azure. Tuttavia, se si utilizza una zona DNS privato di Azure esistente, sarà necessario modificare un file di configurazione.

Requisito per DNS personalizzato

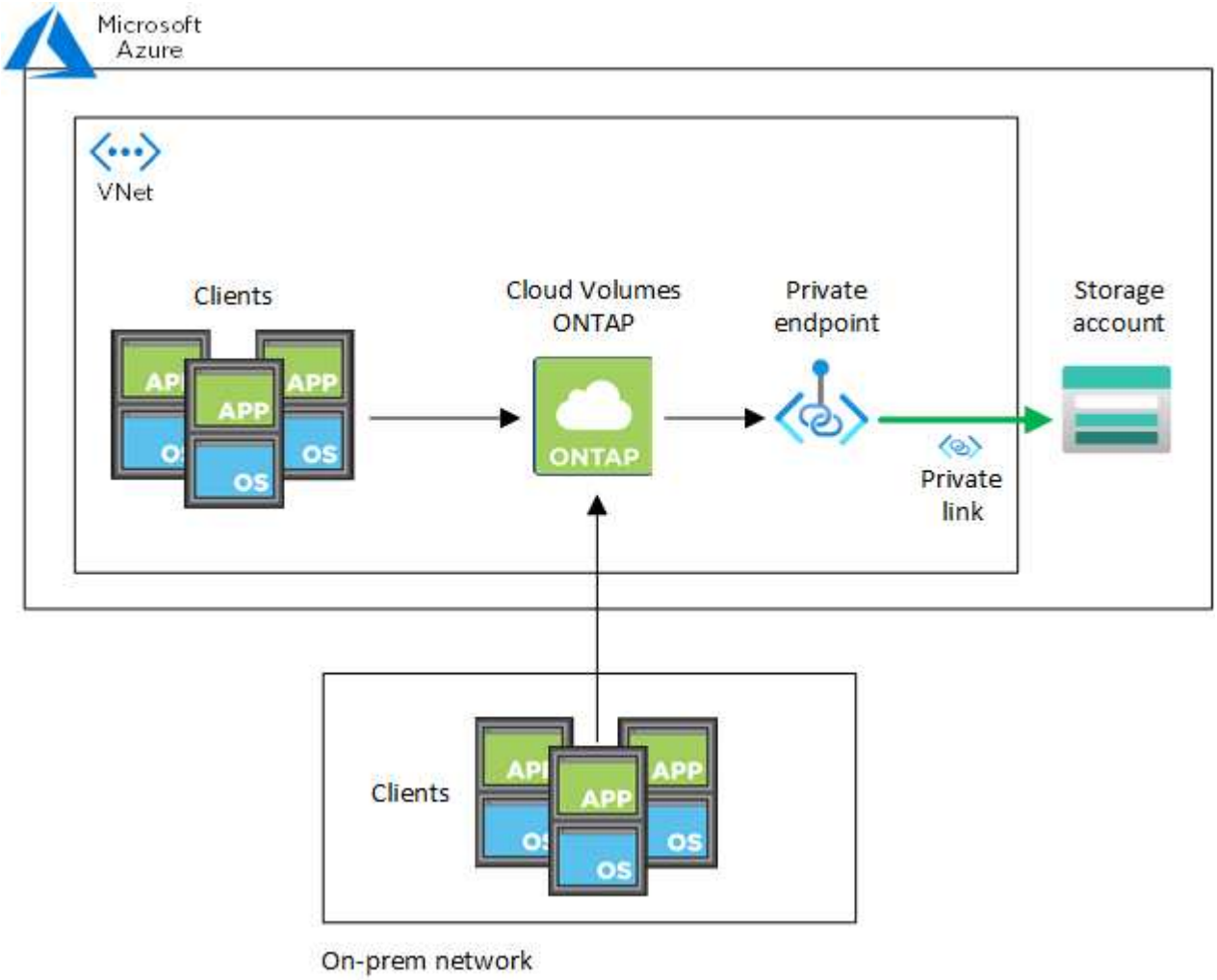
Facoltativamente, se si lavora con DNS personalizzato, è necessario creare un inoltro condizionale alla zona DNS privata di Azure dai server DNS personalizzati. Per saperne di più, fare riferimento a"Documentazione di Azure sull'utilizzo di un inoltro DNS" .

Come funzionano le connessioni Private Link

Quando la console distribuisce Cloud Volumes ONTAP in Azure, crea un endpoint privato nel gruppo di risorse. L'endpoint privato è associato agli account di archiviazione per Cloud Volumes ONTAP. Di conseguenza, l'accesso allo storage Cloud Volumes ONTAP avviene tramite la rete backbone di Microsoft.

L'accesso client avviene tramite collegamento privato quando i client si trovano nella stessa VNet di Cloud Volumes ONTAP, in VNet peering o nella rete locale quando si utilizza una connessione VPN privata o ExpressRoute alla VNet.

Ecco un esempio che mostra l'accesso client tramite un collegamento privato dall'interno della stessa VNet e da una rete locale dotata di una connessione VPN privata o ExpressRoute.



Se l'agente Console e i sistemi Cloud Volumes ONTAP vengono distribuiti in reti virtuali diverse, è necessario configurare il peering tra la rete virtuale in cui è distribuito l'agente Console e la rete virtuale in cui sono distribuiti i sistemi Cloud Volumes ONTAP .

Fornisci dettagli sul tuo DNS privato di Azure

Se usi "DNS privato di Azure" , è necessario modificare un file di configurazione su ciascun agente della console. In caso contrario, la console non può impostare la connessione Azure Private Link tra Cloud Volumes ONTAP e i relativi account di archiviazione associati.

Si noti che il nome DNS deve corrispondere ai requisiti di denominazione DNS di Azure "come mostrato nella documentazione di Azure" .

Passi

1. Eseguire l'SSH sull'host dell'agente della console ed effettuare l'accesso.
2. Vai a `/opt/application/netapp/cloudmanager/docker_occm/data` elenco.
3. Modificare `app.conf` aggiungendo il `user-private-dns-zone-settings` parametro con le seguenti coppie parola chiave-valore:

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

IL `subscription` La parola chiave è obbligatoria solo se la zona DNS privata si trova in un abbonamento diverso da quello dell'agente Console.

4. Salvare il file e disconnettersi dall'agente della console.

   Non è necessario riavviare il computer.

Abilita il rollback in caso di errori

Se la console non riesce a creare un collegamento privato di Azure come parte di azioni specifiche, completa l'azione senza la connessione al collegamento privato di Azure. Ciò può verificarsi quando si crea un nuovo sistema (nodo singolo o coppia HA) o quando si verificano le seguenti azioni su una coppia HA: creazione di un nuovo aggregato, aggiunta di dischi a un aggregato esistente o creazione di un nuovo account di archiviazione quando si superano i 32 TiB.

È possibile modificare questo comportamento predefinito abilitando il rollback se la console non riesce a creare il collegamento privato di Azure. Ciò può contribuire a garantire la piena conformità alle normative di sicurezza della tua azienda.

Se si abilita il rollback, la Console interrompe l'azione e ripristina tutte le risorse create come parte dell'azione.

È possibile abilitare il rollback tramite l'API o aggiornando il file app.conf.

Abilita il rollback tramite l'API

Fare un passo

1. Utilizzare il `PUT /occm/config` Chiamata API con il seguente corpo della richiesta:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Abilita il rollback aggiornando app.conf

Passi

1. Accedere tramite SSH all'host dell'agente della console ed effettuare l'accesso.
2. Passare alla seguente directory: /opt/application/netapp/cloudmanager/docker_occm/data
3. Modifica app.conf aggiungendo il seguente parametro e valore:

```
 "rollback-on-private-link-failure": true
. Salvare il file e disconnettersi dall'agente della console.
```

Non è necessario riavviare il computer.

Spostare un gruppo di risorse di Azure per Cloud Volumes ONTAP nella console di Azure

Cloud Volumes ONTAP supporta gli spostamenti dei gruppi di risorse di Azure, ma il flusso di lavoro avviene solo nella console di Azure.

È possibile spostare un sistema Cloud Volumes ONTAP da un gruppo di risorse a un gruppo di risorse diverso in Azure all'interno della stessa sottoscrizione di Azure. Lo spostamento di gruppi di risorse tra diverse sottoscrizioni di Azure non è supportato.

Passi

1. Rimuovere il sistema Cloud Volumes ONTAP . Fare riferimento a "Rimozione dei sistemi Cloud Volumes ONTAP" .
2. Eseguire lo spostamento del gruppo di risorse nella console di Azure.

   Per completare lo spostamento, fare riferimento a"Spostare le risorse in un nuovo gruppo di risorse o abbonamento nella documentazione di Microsoft Azure" .

3. Nella pagina **Sistemi**, scopri il sistema.
4. Cercare il nuovo gruppo di risorse nelle informazioni del sistema.

Risultato

Il sistema e le sue risorse (VM, dischi, account di archiviazione, interfacce di rete, snapshot) si trovano nel nuovo gruppo di risorse.

Separare il traffico SnapMirror in Azure

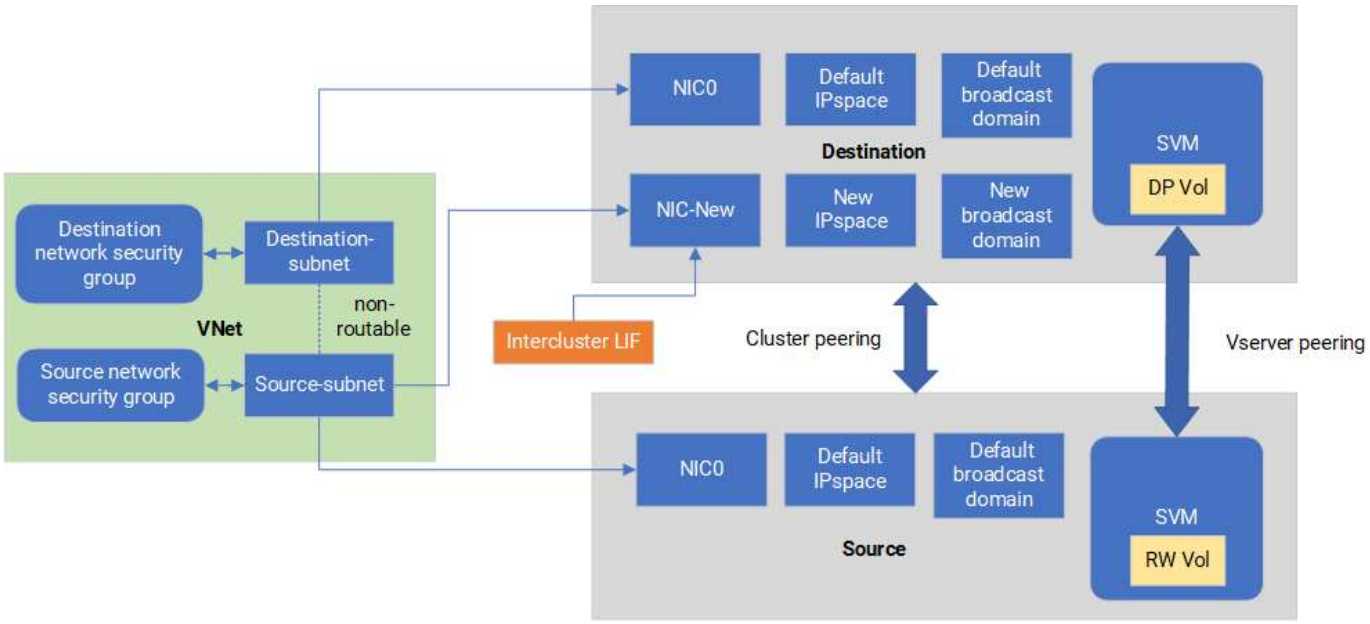
Con Cloud Volumes ONTAP in Azure, puoi separare il traffico di replica SnapMirror dal traffico di dati e di gestione. Per separare il traffico di replica SnapMirror dal traffico dati, è necessario aggiungere una nuova scheda di interfaccia di rete (NIC), un LIF intercluster associato e una subnet non instradabile.

Informazioni sulla segregazione del traffico SnapMirror in Azure

Per impostazione predefinita, la NetApp Console configura tutte le schede di rete e i LIF in una distribuzione Cloud Volumes ONTAP sulla stessa subnet. In tali configurazioni, il traffico di replicazione SnapMirror e il traffico dati e di gestione utilizzano la stessa subnet. La segregazione del traffico SnapMirror sfrutta una subnet aggiuntiva che non è instradabile verso la subnet esistente utilizzata per il traffico dati e di gestione.

Figura 1

I diagrammi seguenti mostrano la segregazione del traffico di replica SnapMirror con una NIC aggiuntiva, un LIF intercluster associato e una subnet non instradabile in una distribuzione a nodo singolo. La distribuzione di una coppia HA differisce leggermente.



Prima di iniziare

Esaminare le seguenti considerazioni:

- È possibile aggiungere una sola scheda di rete a un singolo nodo Cloud Volumes ONTAP o a una distribuzione di coppie HA (istanza VM) per la segregazione del traffico SnapMirror .
- Per aggiungere una nuova NIC, il tipo di istanza VM distribuita deve avere una NIC non utilizzata.
- I cluster di origine e di destinazione devono avere accesso alla stessa rete virtuale (VNet). Il cluster di destinazione è un sistema Cloud Volumes ONTAP in Azure. Il cluster di origine può essere un sistema Cloud Volumes ONTAP in Azure o un sistema ONTAP .

Passaggio 1: creare una scheda di rete aggiuntiva e collegarla alla macchina virtuale di destinazione

Questa sezione fornisce istruzioni su come creare una scheda di rete aggiuntiva e collegarla alla macchina virtuale di destinazione. La VM di destinazione è il sistema a nodo singolo o a coppia HA in Cloud Volumes ONTAP in Azure in cui si desidera configurare la scheda di rete aggiuntiva.

Passi

1. Nella CLI ONTAP , arrestare il nodo.

```
dest::> halt -node <dest_node-vm>
```

2. Nel portale di Azure, verificare che lo stato della VM (nodo) sia arrestato.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Utilizzare l'ambiente Bash in Azure Cloud Shell per arrestare il nodo.
   a. Arrestare il nodo.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. Deallocare il nodo.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. Configurare le regole del gruppo di sicurezza di rete per rendere le due subnet (subnet del cluster di origine e subnet del cluster di destinazione) non instradabili tra loro.
   a. Creare la nuova NIC sulla VM di destinazione.
   b. Cercare l'ID della subnet del cluster di origine.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet -name <vnet> --query id
```

   c. Creare la nuova NIC sulla VM di destinazione con l'ID subnet della subnet del cluster di origine. Qui puoi inserire il nome per la nuova scheda di rete.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

   d. Salvare l'indirizzo IP privato. Questo indirizzo IP, <new_added_nic_primary_addr>, viene utilizzato per creare un LIF intercluster indominio di broadcast, LIF intercluster per la nuova NIC .
5. Collegare la nuova scheda di rete alla macchina virtuale.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. Avviare la VM (nodo).

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. Nel portale di Azure, vai su **Rete** e verifica che la nuova NIC, ad esempio nic-new, esista e che la rete accelerata sia abilitata.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

Per le distribuzioni HA-pair, ripetere i passaggi per il nodo partner.

Passaggio 2: creare un nuovo spazio IP, un dominio di broadcast e un LIF intercluster per la nuova NIC

Uno spazio IP separato per i LIF intercluster fornisce una separazione logica tra le funzionalità di rete per la replica tra cluster.

Utilizzare ONTAP CLI per i passaggi seguenti.

Passi

1. Crea il nuovo IPspace (new_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Creare un dominio broadcast sul nuovo spazio IP (new_ipspace) e aggiungere la porta nic-new.

```
dest::> network port show
```

3. Per i sistemi a nodo singolo, la porta appena aggiunta è *e0b*. Per le distribuzioni a coppia HA con dischi gestiti, la porta appena aggiunta è *e0d*. Per le distribuzioni a coppia HA con page blob, la porta appena aggiunta è *e0e*. Usa il nome del nodo, non il nome della VM. Trova il nome del nodo eseguendo `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Creare un LIF intercluster sul nuovo dominio broadcast (new_bd) e sulla nuova NIC (nic-new).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Verificare la creazione del nuovo LIF intercluster.

```
dest::> net int show
```

Per le distribuzioni HA-pair, ripetere i passaggi per il nodo partner.

Passaggio 3: verificare il peering del cluster tra i sistemi di origine e di destinazione

Questa sezione fornisce istruzioni su come verificare il peering tra i sistemi di origine e di destinazione.

Utilizzare ONTAP CLI per i passaggi seguenti.

Passi

1. Verificare che il LIF intercluster del cluster di destinazione possa effettuare il ping del LIF intercluster del cluster di origine. Poiché il cluster di destinazione esegue questo comando, l'indirizzo IP di destinazione è l'indirizzo IP LIF intercluster sulla sorgente.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Verificare che il LIF intercluster del cluster di origine possa effettuare il ping del LIF intercluster del cluster di destinazione. La destinazione è l'indirizzo IP della nuova NIC creata sulla destinazione.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

Per le distribuzioni HA-pair, ripetere i passaggi per il nodo partner.

Passaggio 4: creare il peering SVM tra il sistema di origine e quello di destinazione

Questa sezione fornisce istruzioni su come creare un peering SVM tra il sistema di origine e quello di destinazione.

Utilizzare ONTAP CLI per i passaggi seguenti.

Passi

1. Creare un cluster peering sulla destinazione utilizzando l'indirizzo IP LIF dell'intercluster di origine come `-peer-addrs` . Per le coppie HA, elencare l'indirizzo IP LIF intercluster di origine per entrambi i nodi come `-peer-addrs` .

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. Inserisci e conferma la passphrase.
3. Creare un cluster peering sulla sorgente utilizzando l'indirizzo IP LIF del cluster di destinazione come `peer-addrs` . Per le coppie HA, elencare l'indirizzo IP LIF intercluster di destinazione per entrambi i nodi come `-peer-addrs` .

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. Inserisci e conferma la passphrase.
5. Verificare che il cluster abbia effettuato il peering.

```
src::> cluster peer show
```

Un peering riuscito mostra **Disponibile** nel campo disponibilità.

6. Creare un peering SVM sulla destinazione. Sia la SVM di origine che quella di destinazione devono essere SVM di dati.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Accetta il peering SVM.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Verificare che l'SVM abbia eseguito il peering.

```
dest::> vserver peer show
```

Spettacoli di stato pari*`peered` * e le applicazioni di peering mostrano*`snapmirror` *.

Passaggio 5: creare una relazione di replica SnapMirror tra il sistema di origine e quello di destinazione

Questa sezione fornisce istruzioni su come creare una relazione di replica SnapMirror tra il sistema di origine e quello di destinazione.

Per spostare una relazione di replica SnapMirror esistente, è necessario prima interrompere la relazione di replica SnapMirror esistente prima di crearne una nuova .

Utilizzare ONTAP CLI per i passaggi seguenti.

Passi

1. Creare un volume dati protetto sulla SVM di destinazione.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Creare la relazione di replica SnapMirror sulla destinazione che include la policy SnapMirror e la pianificazione per la replica.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Inizializza la relazione di replica SnapMirror sulla destinazione.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. Nella CLI ONTAP , convalidare lo stato della relazione SnapMirror eseguendo il seguente comando:

```
dest::> snapmirror show
```

   Lo stato della relazione è `Snapmirrored` e la salute della relazione è `true` .

5. Facoltativo: nella CLI ONTAP , eseguire il seguente comando per visualizzare la cronologia delle azioni per la relazione SnapMirror .

```
dest::> snapmirror show-history
```

Facoltativamente, è possibile montare i volumi di origine e di destinazione, scrivere un file nell'origine e verificare che il volume venga replicato nella destinazione.

Amministrazione di Google Cloud

Modifica il tipo di macchina Google Cloud per Cloud Volumes ONTAP

Quando avvii Cloud Volumes ONTAP in Google Cloud, puoi scegliere tra diversi tipi di macchine. Puoi modificare l'istanza o il tipo di macchina in qualsiasi momento se ritieni che sia sottodimensionato o sovradimensionato per le tue esigenze.

Informazioni su questo compito

- Il giveback automatico deve essere abilitato su una coppia Cloud Volumes ONTAP HA (questa è l'impostazione predefinita). In caso contrario, l'operazione fallirà.

  "Documentazione ONTAP 9: Comandi per la configurazione della restituzione automatica"

- La modifica del tipo di macchina può influire sui costi dei servizi Google Cloud.
- L'operazione riavvia Cloud Volumes ONTAP.

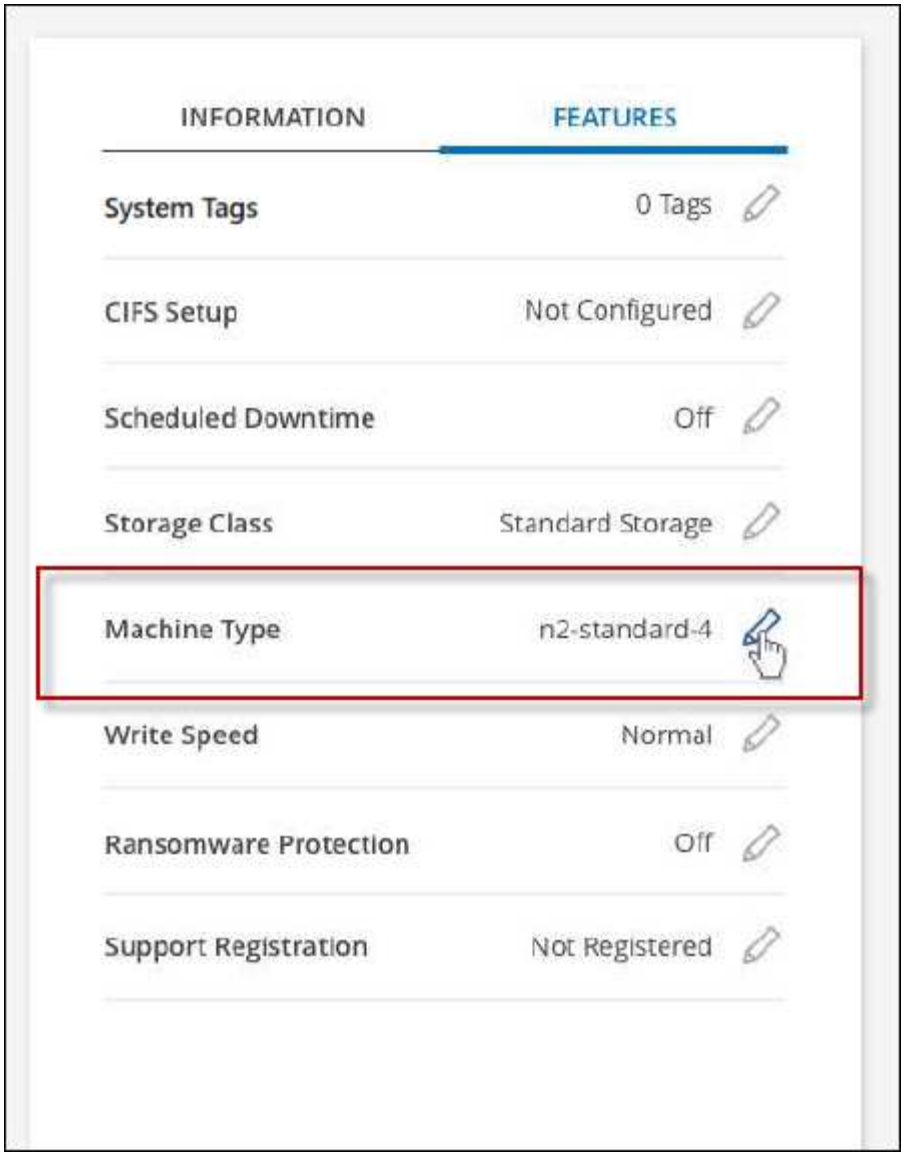
  Per i sistemi a nodo singolo, l'I/O viene interrotto.

  Per le coppie HA, il cambiamento non è dirompente. Le coppie HA continuano a fornire dati.

> La NetApp Console modifica un nodo alla volta avviando l'acquisizione e attendendo la restituzione. Il team di controllo qualità di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha riscontrato alcun problema sul lato client. Con la modifica delle connessioni, sono stati osservati alcuni nuovi tentativi a livello di I/O, ma il livello applicativo ha superato il ricollegamento delle connessioni NFS/CIFS.

Passi

1. Nella pagina **Sistemi**, seleziona il sistema.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **Tipo di macchina**.



Se si utilizza una licenza PAYGO (Node-based pay-as-you-go), è possibile scegliere una licenza e un tipo di macchina diversi facendo clic sull'icona della matita accanto a **Tipo di licenza**.

1. Scegli un tipo di macchina, seleziona la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fai clic su **Modifica**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Convertire le distribuzioni Cloud Volumes ONTAP esistenti in Infrastructure Manager

A partire dal 9 febbraio 2026, le nuove distribuzioni Cloud Volumes ONTAP in Google Cloud potranno utilizzare Google Cloud Infrastructure Manager. Google sta per abbandonare Google Cloud Deployment Manager a favore di Infrastructure Manager. Pertanto, è necessario eseguire manualmente uno strumento di transizione per convertire le distribuzioni Cloud Volumes ONTAP esistenti da Deployment Manager a Infrastructure Manager. Si tratta di una procedura una tantum, al termine della quale i sistemi inizieranno automaticamente a utilizzare Infrastructure Manager.

Informazioni su questo compito

Lo strumento di transizione è disponibile nel "Sito di supporto NetApp" e crea i seguenti artefatti:

- Manufatti Terraform, salvati in `conversion_output/deployment_name`.
- Riepilogo della conversione, salvato in `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`.
- Log di debug, salvati nella `<gcp project number>-<region>-blueprint-config/<cvo name>` directory. Questi log sono necessari per la risoluzione dei problemi. Il `<gcp project number>-<region>-blueprint-config` bucket memorizza i log di Terraform.

> I sistemi Cloud Volumes ONTAP che utilizzano Infrastructure Manager archiviano dati e record nei bucket di Google Cloud Storage. L'utilizzo di questi bucket potrebbe comportare costi aggiuntivi, ma non modificare o eliminare i bucket o il loro contenuto:
>
> - `gs://netapp-cvo-infrastructure-manager-<project id>`: per le versioni ONTAP e i modelli SVM Terraform utilizzati per le nuove distribuzioni di Cloud Volumes ONTAP. Al suo interno, il bucket `dm-to-im-convert` contiene i file Terraform di Cloud Volumes ONTAP.
> - `<gcp project number>-<region>-blueprint-config`: per l'archiviazione degli artefatti Google Cloud Terraform.

Prima di iniziare

- Assicurati che il tuo sistema Cloud Volumes ONTAP sia 9.16.1 o successivo.
- Assicurarsi che nessuna delle risorse Cloud Volumes ONTAP o delle relative proprietà sia stata modificata manualmente da Google Cloud Console.
- Assicurati che le API di Google Cloud siano abilitate. Fai riferimento a "Abilita le API di Google Cloud". Assicurati che, insieme alle altre API, sia abilitata anche la Google Cloud Quotas API.
- Verificare che l'account di servizio dell'agente della NetApp Console disponga di tutte le autorizzazioni necessarie. Fare riferimento a "Autorizzazioni di Google Cloud per l'agente della console".

  Per le distribuzioni in modalità privata, assicurarsi dei seguenti prerequisiti aggiuntivi:

  - Assicurati di disporre della versione più recente dell'agente Console. Scarica il programma di installazione del prodotto dal NetApp Support Site e quindi installa manualmente l'agente sul tuo host in modo che l'agente possa utilizzare le API di Infrastructure Manager.
  - Se esegui lo strumento in modalità privata, assicurati che, insieme alle altre API, tu abbia abilitato l'API Cloud Build. "Abilita le API di Google Cloud".
  - Assicurarsi di aver completato le configurazioni di rete e creato il pool di worker per le distribuzioni in modalità privata. Fare riferimento a "Configurazione di Infrastructure Manager per distribuzioni in modalità privata".

- Lo strumento di conversione utilizza i seguenti domini. Abilitali sulla porta 443 nella tua rete:

Dominio	Porta	Protocollo	Direzione	Scopo
cloudresourcemanager.googleapis.com	443	TCP	USCITA	Validazione del progetto

Dominio	Porta	Protocollo	Direzione	Scopo
deploymentmanager.googleapis.com	443	TCP	USCITA	Scoperta della distribuzione
Chiamate API di compute utilizzate da Google Cloud e Terraform Import and Plan	443	TCP	USCITA	API di Infrastructure Manager
storage.googleapis.com	443	TCP	USCITA	Operazioni bucket GCS
iam.googleapis.com	443	TCP	USCITA	Convalida dell'account di servizio
compute.googleapis.com	443	TCP	USCITA	Chiamate API di compute utilizzate da Google Cloud e Terraform Import and Plan
cloudbuild.googleapis.com	443	TCP	USCITA	Operazioni di build richieste solo per la modalità privata
openidconnect.googleapis.com	443	TCP	USCITA	Autenticazione
oauth2.googleapis.com	443	TCP	USCITA	Scambio di token OAuth2
registry.terraform.io	443	TCP	USCITA	Registro dei provider Terraform
releases.hashicorp.com	443	TCP	USCITA	Download binari di Terraform
apt.releases.hashicorp.com	443	TCP	USCITA	Repository APT HashiCorp
us-central1-docker.pkg.dev	443	TCP	USCITA	GCP Artifact Registry
metadata.google.internal	80	HTTP	Interno	Metadati VM e token di autenticazione
pypi.org	443	TCP	USCITA	Indice dei pacchetti Python
files.pythonhosted.org	443	TCP	USCITA	Download dei pacchetti Python
checkpoint-api.hashicorp.com	443	TCP	USCITA	Verifica della versione di Terraform
download.docker.com	443	TCP	USCITA	repository APT Docker
security.ubuntu.com	80/443	TCP	USCITA	Aggiornamenti di sicurezza Ubuntu

Dominio	Porta	Protocollo	Direzione	Scopo
*.gce.archive.ubuntu.com	80	TCP	USCITA	Mirror dei pacchetti Ubuntu

Prepara l'ambiente per l'esecuzione dello strumento

Eseguire questi passaggi prima di eseguire lo strumento.

Passi

1. Crea un ruolo e associalo a un account di servizio:
   a. Crea un file YAML con le seguenti autorizzazioni:

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

Includi autorizzazioni aggiuntive per le distribuzioni in modalità privata

> Se si esegue lo strumento in modalità privata, aggiungere l `cloudbuild.workerpools.get`autorizzazione anche al file YAML.

b. Crea un ruolo personalizzato in Google Cloud con le autorizzazioni definite nel file YAML. `gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \ --file=YAML_FILE_PATH` Per ulteriori informazioni, consulta "Creazione e gestione di ruoli personalizzati".

c. Collega il ruolo personalizzato all'account di servizio che utilizzerai per creare la VM.

d. Aggiungi il `roles/iam.serviceAccountUser` ruolo a questo account di servizio. Fai riferimento a "Panoramica degli account di servizio".

2. Crea una VM con le seguenti configurazioni. Esegui lo strumento su questa VM.
   - Tipo di macchina: Google Compute Engine machine type e2-medium
   - OS: in base alle tue esigenze, seleziona una di queste immagini:
     - Ubuntu 25.10 AMD64 Minimal (immagine: ubuntu-minimal-2510-amd64)
     - SUSE Linux Enterprise Server 15 SP7 x86_64
   - Networking: Firewall che consente HTTP e HTTPs
   - Dimensione del disco: 20GB
   - Sicurezza: Account di servizio: l'account di servizio che hai creato
   - Sicurezza: Ambito di accesso - accesso impostato per ciascuna API:
     - Piattaforma cloud: abilitato
     - Compute Engine: sola lettura
     - Storage: sola lettura (predefinita)
     - Google Cloud Logging (in precedenza Stackdriver Logging) API: solo scrittura (predefinita)
     - Stackdriver Monitoring (ora parte di Google Cloud Operations) API: solo scrittura (predefinita)
     - Gestione dei servizi: sola lettura (predefinita)
     - Controllo del servizio: abilitato (predefinito)
     - Google Cloud Trace (previously Stackdriver Trace): solo scrittura (predefinito)
3. Connetti alla nuova VM utilizzando SSH: `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. Scarica lo strumento di conversione da "Sito di supporto NetApp" utilizzando le tue credenziali NSS: `wget <download link from NetApp Support site>`
5. Estrai il file TAR scaricato: `unzip <downloaded file name>`

Ubuntu

1. Scarica e installa questi pacchetti prerequisiti:
   - Docker: 28.2.2 build 28.2.2-0ubuntu1 o successiva
   - Terraform: 1.14.1 o successivo
   - Python: 3.13.7, python3-pip, python3 venv

   ```
   sudo apt-get update
   sudo apt-get install python3-pip python3-venv -y
   wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg
   --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
   https://apt.releases.hashicorp.com noble main" | sudo tee
   /etc/apt/sources.list.d/hashicorp.list
   sudo apt update && sudo apt install terraform
   sudo apt-get install -y docker.io
   sudo systemctl start docker
   ```

   Google Cloud CLI `gcloud` è preinstallato sulla VM.

SUSE Linux Enterprise Server

1. Imposta Python: `sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 2`
2. Installa pip3 per installare il pacchetto: `python3.11 -m ensurepip --upgrade`
3. Installa Terraform:

   ```
   wget
   https://releases.hashicorp.com/terraform/1.7.4/terraform_1.7.4_linux
   _amd64.zip
   unzip terraform_1.7.4_linux_amd64.zip
   sudo mv terraform /usr/local/bin/
   rm terraform_1.7.4_linux_amd64.zip
   ```

4. Installa Google Cloud SDK (gcloud)

   ```
   curl https://sdk.cloud.google.com | bash
   exec -l $SHELL
   ```

Esegui lo strumento di conversione

Questi passaggi sono validi sia per Ubuntu che per SUSE Linux Enterprise Server per l'esecuzione dello strumento di conversione.

Passi

1. Aggiungi l'utente corrente al gruppo Docker, in modo che lo strumento possa utilizzare Docker senza `sudo` privilegi.

   ```
   sudo usermod -aG docker $USER
   newgrp docker
   ```

2. Installa lo strumento di conversione:

   ```
   cd <folder where you extracted the tool>
    ./install.sh
   ```

   In questo modo lo strumento viene installato in un ambiente isolato, `dmconvert-venv` e viene verificato che tutti i pacchetti software richiesti siano installati.

3. Immettere l'ambiente in cui è installato lo strumento: `source dmconvert-venv/bin/activate`
4. Eseguire lo strumento di conversione come `non-sudo`utente. Assicurarsi di utilizzare lo stesso account di servizio dell'account di servizio dell'agente della Console e che l'account di servizio disponga di tutti i "autorizzazioni necessarie per Google Cloud Infrastructure Manager".

   ```
   dmconvert \
   --project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
   deployment> \
   --cvo-name=<Cloud Volumes ONTAP system name> \
   --service-account=<the service account attached to the Console agent>
   ```

Esegui lo strumento in distribuzioni in modalità privata

Specificare il `--worker-pool` parametro per eseguire lo strumento nelle distribuzioni in modalità privata. Per la configurazione del pool di worker, fare riferimento a "Configurazione di Infrastructure Manager per distribuzioni in modalità privata".

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes
ONTAP deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console
agent> \
--worker-pool=<worker pool name>
```

Dopo aver finito

Lo strumento visualizza un elenco di tutti i sistemi Cloud Volumes ONTAP e i dettagli delle SVM. Al termine dell'esecuzione, puoi vedere lo stato di tutti i sistemi convertiti. Ogni sistema convertito appare nella Google Console sotto Infrastructure Manager in un formato *<system-name-imdeploy>*, indicando che la Console ora utilizza le API di Infrastructure Manager per gestire quel sistema Cloud Volumes ONTAP.

> Dopo la conversione, non eliminare l'oggetto di distribuzione per Deployment Manager nella Google Cloud Console. Questo oggetto di distribuzione contiene informazioni che potrebbero essere necessarie per eseguire il rollback del sistema convertito.

Se è necessario annullare la conversione, è necessario utilizzare la stessa VM. Se sono stati convertiti tutti i sistemi e non è necessario annullare la conversione a Deployment Manager, è possibile eliminare la VM.

Ripristina la conversione

Se non vuoi continuare con la conversione, puoi tornare a Deployment Manager seguendo questi passaggi:

Passi

1. Sullo stesso VM che hai creato per l'esecuzione dello strumento, esegui questo comando:

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. Attendi fino al completamento del rollback.

Link correlati

- "NetApp Console Agent 4.2.0 Note sulla versione"

- "Autorizzazioni richieste per Google Cloud Infrastructure Manager"

Amministrare Cloud Volumes ONTAP utilizzando System Manager

Le funzionalità avanzate di gestione dello storage in Cloud Volumes ONTAP sono disponibili tramite ONTAP System Manager, un'interfaccia di gestione fornita con i sistemi ONTAP . È possibile accedere a System Manager direttamente dalla NetApp Console.

Caratteristiche

È possibile eseguire varie funzioni di gestione dell'archiviazione utilizzando ONTAP System Manager nella Console. L'elenco seguente include alcune di queste funzionalità, sebbene non sia esaustivo:

- Gestione avanzata dell'archiviazione: gestione di gruppi di coerenza, condivisioni, qtree, quote e VM di archiviazione.
- Spostamento del volume: "Spostare un volume su un aggregato diverso."
- Gestione della rete: gestione di spazi IP, interfacce di rete, set di porte e porte Ethernet.
- Gestisci volumi FlexGroup : puoi creare e gestire volumi FlexGroup solo tramite System Manager. La console non supporta la creazione di volumi FlexGroup .
- Eventi e processi: visualizza registri eventi, avvisi di sistema, processi e registri di controllo.
- Protezione avanzata dei dati: proteggi le VM di storage, le LUN e i gruppi di coerenza.
- Gestione host: configurazione di gruppi di iniziatori SAN e client NFS.
- Gestione dello storage a oggetti ONTAP S3: le funzionalità di gestione dello storage ONTAP S3 in Cloud Volumes ONTAP sono disponibili solo in System Manager e non nella Console.

Configurazioni supportate

- La gestione avanzata dell'archiviazione tramite ONTAP System Manager è disponibile in Cloud Volumes ONTAP 9.10.0 e versioni successive nelle regioni cloud standard.
- L'integrazione di System Manager non è supportata nelle regioni GovCloud o nelle regioni che non dispongono di accesso a Internet in uscita.

Limitazioni

Alcune funzionalità visualizzate nell'interfaccia di System Manager non sono supportate da Cloud Volumes ONTAP:

- NetApp Cloud Tiering: Cloud Volumes ONTAP non supporta Cloud Tiering. È consigliabile impostare la suddivisione in livelli dei dati nell'archiviazione degli oggetti direttamente dalla Visualizzazione standard durante la creazione dei volumi.
- Livelli: la gestione degli aggregati (inclusi i livelli locali e cloud) non è supportata da System Manager. È necessario gestire gli aggregati direttamente dalla Vista standard.
- Aggiornamenti del firmware: Cloud Volumes ONTAP non supporta gli aggiornamenti automatici del firmware dalla pagina **Cluster > Impostazioni** di System Manager.
- Controllo degli accessi basato sui ruoli: il controllo degli accessi basato sui ruoli da System Manager non è supportato.
- Disponibilità continua SMB (CA): Cloud Volumes ONTAP non supporta "azioni SMB continuamente disponibili" per operazioni non distruttive.

Configurare l’autenticazione per l’accesso a System Manager

In qualità di amministratore, puoi attivare l’autenticazione per gli utenti che accedono a ONTAP System Manager dalla Console. È possibile determinare il livello corretto di autorizzazioni di accesso in base ai ruoli utente ONTAP e abilitare o disabilitare l’autenticazione in base alle esigenze. Se si abilita l’autenticazione, gli utenti dovranno immettere le proprie credenziali utente ONTAP ogni volta che accedono a System Manager dalla Console o quando la pagina viene ricaricata, perché la Console non memorizza le credenziali internamente. Se si disabilita l’autenticazione, gli utenti possono accedere a System Manager utilizzando le credenziali di amministratore.

Questa impostazione è applicabile a ciascun agente della console per gli utenti ONTAP nella tua organizzazione o nel tuo account, indipendentemente dal sistema Cloud Volumes ONTAP .

Autorizzazioni richieste

Per modificare le impostazioni dell’agente della console per l’autenticazione utente Cloud Volumes ONTAP , è necessario disporre dei privilegi di amministratore dell’organizzazione o dell’account.

Passi

1. Dal riquadro di navigazione a sinistra, vai su **Amministrazione > Agenti**.
2. Fare clic su icona per l’agente Console richiesto e selezionare **Modifica agente Console**.
3. In **Forza credenziali utente**, seleziona la casella di controllo **Abilita/Disabilita**. Per impostazione predefinita, l’autenticazione è disabilitata.

   Se si imposta questo valore su **Abilita**, l’autenticazione viene reimpostata e sarà necessario modificare tutti i flussi di lavoro esistenti per adattarli a questa modifica.

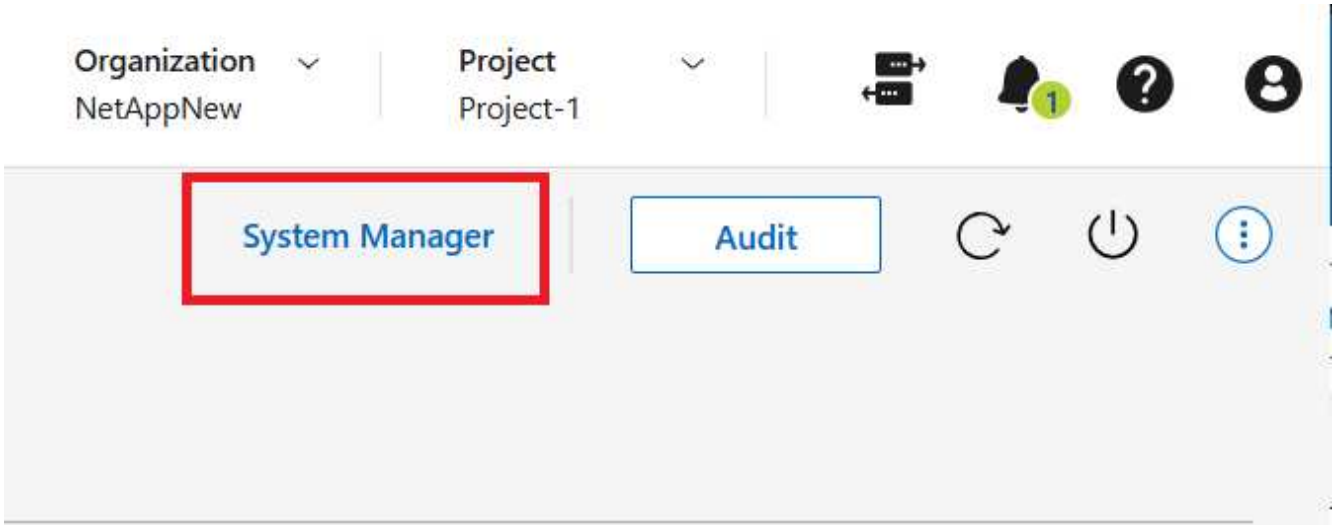
4. Fare clic su **Salva**.

Inizia con System Manager

È possibile accedere a ONTAP System Manager da un sistema Cloud Volumes ONTAP .

Passi

1. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
2. Nella pagina **Sistemi**, fare doppio clic sul sistema Cloud Volumes ONTAP richiesto.
3. Fare clic su **Gestione sistema**.



4. Se richiesto, inserisci le tue credenziali utente ONTAP e fai clic su **Accedi**.
5. Se appare un messaggio di conferma, leggerlo attentamente e fare clic su **Chiudi**.

Utilizza System Manager per gestire il tuo sistema Cloud Volumes ONTAP . Puoi cliccare su **Torna indietro** per tornare alla Console.

Aiuto con l'utilizzo di System Manager

Se hai bisogno di aiuto nell'utilizzo di System Manager con Cloud Volumes ONTAP, puoi fare riferimento a "Documentazione ONTAP" per istruzioni dettagliate. Ecco alcuni link alla documentazione ONTAP che potrebbero esserti utili:

- "Ruoli, applicazioni e autenticazione ONTAP"
- "Utilizzare System Manager per accedere a un cluster" .
- "Gestione del volume e LUN"
- "Gestione della rete"
- "Protezione dei dati"
- "Crea condivisioni SMB costantemente disponibili"

Amministra Cloud Volumes ONTAP dalla CLI

Cloud Volumes ONTAP CLI consente di eseguire tutti i comandi amministrativi ed è una buona scelta per attività avanzate o se si ha più dimestichezza con l'utilizzo della CLI. È possibile connettersi alla CLI tramite Secure Shell (SSH).

Prima di iniziare

L'host da cui si utilizza SSH per connettersi a Cloud Volumes ONTAP deve disporre di una connessione di rete a Cloud Volumes ONTAP. Ad esempio, potrebbe essere necessario effettuare una connessione SSH da un jump host presente nella rete del tuo provider cloud.

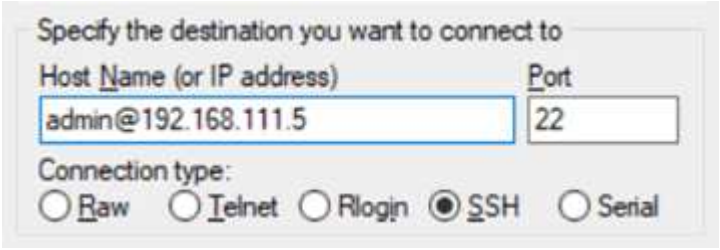
Se distribuite in più AZ, le configurazioni Cloud Volumes ONTAP HA utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che faccia parte dello stesso dominio di routing.

Passi

1. Nella NetApp Console, identificare l'indirizzo IP dell'interfaccia di gestione del cluster:
   a. Dal menu di navigazione a sinistra, seleziona **Archiviazione > Gestione**.
   b. Nella pagina **Sistemi**, selezionare il sistema Cloud Volumes ONTAP .
   c. Copiare l'indirizzo IP di gestione del cluster visualizzato nel riquadro di destra.
2. Utilizzare SSH per connettersi all'indirizzo IP dell'interfaccia di gestione del cluster utilizzando l'account amministratore.

   Esempio

   L'immagine seguente mostra un esempio che utilizza PuTTY:

3. Al prompt di accesso, immettere la password per l'account amministratore.

   Esempio

   ```
   Password: ********
   COT2::>
   ```

Stato di salute e eventi del sistema

Verifica la configurazione AutoSupport per Cloud Volumes ONTAP

AutoSupport monitora in modo proattivo lo stato di salute del tuo sistema e invia messaggi al supporto tecnico NetApp . Per impostazione predefinita, AutoSupport è abilitato su ciascun nodo per inviare messaggi al supporto tecnico tramite il protocollo di trasporto HTTPS. È meglio verificare che AutoSupport possa inviare questi messaggi.

L'unico passaggio di configurazione richiesto è garantire che Cloud Volumes ONTAP disponga di connettività Internet in uscita. Per maggiori dettagli, fare riferimento ai requisiti di rete del proprio provider cloud.

Requisiti AutoSupport

I nodi Cloud Volumes ONTAP richiedono l'accesso a Internet in uscita per NetApp AutoSupport, che monitora in modo proattivo lo stato del sistema e invia messaggi al supporto tecnico NetApp .

I criteri di routing e firewall devono consentire il traffico HTTPS verso i seguenti endpoint affinché Cloud Volumes ONTAP possa inviare messaggi AutoSupport :

- \ https://mysupport.netapp.com/aods/asupmessage

- \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup

Se non è disponibile una connessione Internet in uscita per inviare messaggi AutoSupport , la NetApp Console configura automaticamente i sistemi Cloud Volumes ONTAP per utilizzare l'agente della console come server proxy. L'unico requisito è assicurarsi che il gruppo di sicurezza dell'agente Console consenta connessioni *in entrata* sulla porta 3128. Sarà necessario aprire questa porta dopo aver distribuito l'agente Console.

Se hai definito regole in uscita rigorose per Cloud Volumes ONTAP, dovrai anche assicurarti che il gruppo di sicurezza Cloud Volumes ONTAP consenta connessioni *in uscita* sulla porta 3128.

Se si utilizza una coppia HA, il mediatore HA non richiede l'accesso a Internet in uscita.

Dopo aver verificato che l'accesso a Internet in uscita è disponibile, puoi testare AutoSupport per assicurarti che possa inviare messaggi. Per le istruzioni, fare riferimento al "Documentazione ONTAP : configurazione di AutoSupport" .

Risolvi i problemi di configurazione AutoSupport

Se non è disponibile una connessione in uscita e la Console non riesce a configurare il sistema Cloud Volumes ONTAP per utilizzare l'agente della Console come server proxy, la Console ti invierà una notifica che ti informa che il sistema non è in grado di inviare messaggi AutoSupport . Per risolvere il problema, seguire questi passaggi.

Passi

1. Connettersi in modo sicuro (tramite SSH) al sistema Cloud Volumes ONTAP per utilizzare ONTAP CLI.

   "Scopri come effettuare l'SSH su Cloud Volumes ONTAP" .

2. Controllare lo stato dettagliato del sottosistema AutoSupport :

   ```
   autosupport check show-details
   ```

   La risposta è la seguente:

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

Se lo stato della categoria http-https è `OK` significa che AutoSupport è configurato correttamente e che i messaggi possono essere inviati.

3. In caso contrario, verificare l'URL proxy per ciascun nodo Cloud Volumes ONTAP :

   ```
   autosupport show -fields proxy-url
   ```

4. Se il parametro URL proxy è vuoto, configurare Cloud Volumes ONTAP per utilizzare l'agente Console come proxy:

   ```
   autosupport modify -proxy-url http://<console agent private ip>:3128
   ```

5. Verificare nuovamente lo stato AutoSupport :

   ```
   autosupport check show-details
   ```

6. Se lo stato è ancora fallito, convalidare la connettività tra Cloud Volumes ONTAP e l'agente della console sulla porta `3128`.
7. Se dopo la verifica lo stato risulta ancora fallito, effettuare l'accesso SSH all'agente della console.

   "Scopri di più sulla connessione alla VM Linux per l'agente della console"

8. Vai a `/opt/application/netapp/cloudmanager/docker_occm/data/`.
9. Aprire il file di configurazione del proxy `squid.conf`. Questa è la struttura del file:

```
http_port 3128
acl netapp_support dst support.netapp.com
http_access allow netapp_support
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

10. Se il file non contiene una voce per il blocco CIDR del sistema Cloud Volumes ONTAP , aggiungere una nuova voce e consentire l'accesso:

    ```
    acl cvonet src <cidr>

    http_access allow cvonet
    ```

    Ecco un esempio:

```
http_port 3128
acl netapp_support dst support.netapp.com
acl cvonet src <cidr>
http_access allow netapp_support
http_access allow cvonet
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

11. Dopo aver modificato il file di configurazione, riavviare il contenitore proxy come `sudo`. Quindi, a seconda che tu stia utilizzando Docker o Podman, esegui questi comandi:

    Per Docker, esegui `docker restart squid`.

    Se stai usando Podman, esegui `podman restart squid`.

12. Tornare alla CLI ONTAP e verificare che Cloud Volumes ONTAP possa inviare messaggi AutoSupport :

    ```
    autosupport check show-details
    ```

Link correlati

- "Requisiti di rete per Cloud Volumes ONTAP in AWS"
- "Requisiti di rete per Cloud Volumes ONTAP in Azure"
- "Requisiti di rete per Cloud Volumes ONTAP in Google Cloud"

Configurare EMS per i sistemi Cloud Volumes ONTAP

Il sistema di gestione degli eventi (EMS) raccoglie e visualizza informazioni sugli eventi che si verificano sui sistemi ONTAP . Per ricevere notifiche sugli eventi, è possibile impostare destinazioni degli eventi (indirizzi e-mail, host trap SNMP o server syslog) e percorsi degli eventi per una particolare gravità dell'evento.

È possibile configurare EMS tramite la CLI. Per le istruzioni, fare riferimento al "Documentazione ONTAP : panoramica della configurazione EMS" .

Concetti

Licenza

Licenze per Cloud Volumes ONTAP

Sono disponibili diverse opzioni di licenza per Cloud Volumes ONTAP. Ogni opzione ti consente di scegliere il modello di consumo più adatto alle tue esigenze.

Panoramica delle licenze

Per i nuovi clienti sono disponibili le seguenti opzioni di licenza.

Licenza basata sulla capacità
: Paga più sistemi Cloud Volumes ONTAP nel tuo account NetApp in base alla capacità fornita. Include la possibilità di acquistare servizi aggiuntivi di dati cloud. Per ulteriori informazioni sui modelli di consumo o sulle opzioni di acquisto nelle licenze basate sulla capacità, fare riferimento a"Scopri di più sulle licenze basate sulla capacità" .

Abbonamento Keystone
: Un servizio basato su abbonamento con pagamento in base alla crescita che offre un'esperienza cloud ibrida senza interruzioni per coppie ad alta disponibilità (HA).

Le sezioni seguenti forniscono maggiori dettagli su ciascuna di queste opzioni.

Non è disponibile supporto per l'utilizzo di funzionalità concesse in licenza senza licenza.

Licenza basata sulla capacità

I pacchetti di licenze basati sulla capacità consentono di pagare Cloud Volumes ONTAP per TiB di capacità. La licenza è associata al tuo account NetApp e ti consente di addebitare la licenza su più sistemi, a condizione che la licenza disponga di capacità sufficiente.

Ad esempio, è possibile acquistare una singola licenza da 20 TiB, distribuire quattro sistemi Cloud Volumes ONTAP e quindi allocare un volume da 5 TiB a ciascun sistema, per un totale di 20 TiB. La capacità è disponibile per i volumi su ciascun sistema Cloud Volumes ONTAP distribuito in quell'account.

La licenza basata sulla capacità è disponibile sotto forma di *pacchetto*. Quando distribuisci un sistema Cloud Volumes ONTAP , puoi scegliere tra diversi pacchetti di licenze in base alle tue esigenze aziendali.

Sebbene l'utilizzo effettivo e la misurazione dei prodotti e dei servizi gestiti nella NetApp Console siano sempre calcolati in GiB e TiB, i termini GB/GiB e TB/TiB vengono utilizzati in modo intercambiabile. Ciò si riflette negli elenchi del Cloud Marketplace, nei preventivi di prezzo, nelle descrizioni degli elenchi e in altra documentazione di supporto.

Pacchetti

Per Cloud Volumes ONTAP sono disponibili i seguenti pacchetti basati sulla capacità. Per ulteriori informazioni sui pacchetti di licenze basati sulla capacità, fare riferimento a"Scopri di più sulle licenze basate sulla capacità" .

Per un elenco dei tipi di VM supportati con i seguenti pacchetti basati sulla capacità, fare riferimento a:

- "Configurazioni supportate in Azure"
- "Configurazioni supportate in Google Cloud"

Freemium

Fornisce gratuitamente tutte le funzionalità Cloud Volumes ONTAP di NetApp (si applicano comunque i costi del provider cloud). Un pacchetto Freemium ha le seguenti caratteristiche:

- Non è necessaria alcuna licenza o contratto.
- Il supporto di NetApp non è incluso.
- La capacità fornita è limitata a 500 GiB per sistema Cloud Volumes ONTAP .
- Con l'offerta Freemium puoi utilizzare fino a 10 sistemi Cloud Volumes ONTAP per account NetApp , per qualsiasi provider cloud.
- Se la capacità fornita per un sistema Cloud Volumes ONTAP supera i 500 GiB, la Console converte il sistema in un pacchetto Essentials.

  Non appena un sistema viene convertito nel pacchetto Essentials,"tariffa minima" si applica ad esso.

  Un sistema Cloud Volumes ONTAP convertito in un pacchetto Essentials non può essere riportato a Freemium anche se la capacità fornita viene ridotta a meno di 500 GiB. Altri sistemi con capacità di provisioning inferiore a 500 GiB restano su Freemium (purché siano stati distribuiti utilizzando l'offerta Freemium).

Essenziali

È possibile pagare in base alla capacità in diverse configurazioni:

- Scegli la configurazione Cloud Volumes ONTAP :
  - Un singolo nodo o sistema HA
  - Archiviazione di file e blocchi o dati secondari per il ripristino di emergenza (DR)
- Aggiungi uno qualsiasi dei servizi dati cloud di NetApp a un costo aggiuntivo

Professionale

Paga in base alla capacità per qualsiasi tipo di configurazione Cloud Volumes ONTAP con backup illimitati.

- Fornisce licenze per qualsiasi configurazione Cloud Volumes ONTAP

  Nodo singolo o HA con addebito della capacità per volumi primari e secondari alla stessa tariffa

- Include backup di volumi illimitati tramite NetApp Backup and Recovery, ma solo per i sistemi Cloud Volumes ONTAP che utilizzano il pacchetto Professional.

> Per il backup e il ripristino è richiesto un abbonamento pay-as-you-go (PAYGO); tuttavia, non verranno addebitati costi per l'utilizzo di questo servizio. Per ulteriori informazioni sulla configurazione delle licenze per Backup e Ripristino, fare riferimento a "Impostare la licenza per il backup e il ripristino" .

- Aggiungi uno qualsiasi dei servizi dati cloud di NetApp a un costo aggiuntivo

Disponibilità di licenze basate sulla capacità

Per rendere disponibili le licenze PAYGO e BYOL per i sistemi Cloud Volumes ONTAP è necessario che l'agente Console sia attivo e funzionante.

"Scopri di più sugli agenti della console" .

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAPP" .

Come iniziare

Scopri come iniziare a utilizzare le licenze basate sulla capacità:

- "Impostare le licenze per Cloud Volumes ONTAP in AWS"
- "Configurare le licenze per Cloud Volumes ONTAP in Azure"
- "Impostare le licenze per Cloud Volumes ONTAP in Google Cloud"

Abbonamento Keystone

Un servizio basato su abbonamento con pagamento in base alla crescita che offre un'esperienza cloud ibrida senza interruzioni per coloro che preferiscono modelli di consumo OpEx a CapEx anticipati o leasing.

La tariffazione si basa sulla dimensione della capacità impegnata per una o più coppie Cloud Volumes ONTAP HA nel tuo abbonamento Keystone .

La capacità fornita per ciascun volume viene aggregata e confrontata periodicamente con la capacità impegnata nel tuo abbonamento Keystone e qualsiasi eccedenza viene addebitata come burst nel tuo abbonamento Keystone .

"Scopri di più su NetApp Keystone" .

Configurazioni supportate

Gli abbonamenti Keystone sono supportati con coppie HA. Questa opzione di licenza non è supportata con sistemi a nodo singolo.

Limite di capacità

Nel modello di licenza basato sulla capacità, ogni sistema Cloud Volumes ONTAP supporta la suddivisione in livelli per l'archiviazione di oggetti e la capacità totale suddivisa in livelli può essere scalata fino al limite del bucket del provider cloud. Sebbene la licenza non imponga restrizioni di capacità, seguire le "Migliori pratiche FabricPool" per garantire prestazioni ottimali, affidabilità ed efficienza dei costi durante la configurazione e la gestione del tiering.

Per informazioni sui limiti di capacità di ciascun provider cloud, fare riferimento alla relativa documentazione:

- "Documentazione AWS"
- "Documentazione di Azure per i dischi gestiti"E "Documentazione di Azure per l'archiviazione BLOB"
- "Documentazione di Google Cloud"

Come iniziare

Scopri come iniziare con un abbonamento Keystone :

- "Impostare le licenze per Cloud Volumes ONTAP in AWS"
- "Configurare le licenze per Cloud Volumes ONTAP in Azure"
- "Impostare le licenze per Cloud Volumes ONTAP in Google Cloud"

Licenza basata sui nodi

La licenza basata sui nodi è il modello di licenza della generazione precedente che consentiva di concedere in licenza Cloud Volumes ONTAP per nodo. Questo modello di licenza non è disponibile per i nuovi clienti. La ricarica per nodo è stata sostituita dai metodi di ricarica per capacità descritti sopra.

NetApp ha pianificato la fine della disponibilità (EOA) e del supporto (EOS) delle licenze basate sui nodi. Dopo l'EOA e l'EOS, le licenze basate sui nodi dovranno essere convertite in licenze basate sulla capacità.

Per informazioni, fare riferimento a "Comunicato al cliente: CPC-00589" .

Fine della disponibilità delle licenze basate sui nodi

A partire dall'11 novembre 2024, la disponibilità limitata delle licenze basate sui nodi è terminata. Il supporto per le licenze basate sui nodi termina il 31 dicembre 2024.

Se disponi di un contratto valido basato su nodi che si estende oltre la data EOA, puoi continuare a utilizzare la licenza fino alla scadenza del contratto. Una volta scaduto il contratto, sarà necessario passare al modello di licenza basato sulla capacità. Se non si dispone di un contratto a lungo termine per un nodo Cloud Volumes ONTAP , è importante pianificare la conversione prima della data di fine del supporto.

Per saperne di più su ciascun tipo di licenza e sull'impatto dell'EOA su di esso, consulta questa tabella:

Tipo di licenza	Impatto dopo l'EOA
Licenza valida basata su nodi acquistata tramite Bring Your Own License (BYOL)	La licenza rimane valida fino alla scadenza. Le licenze basate su nodi non utilizzate esistenti possono essere utilizzate per distribuire nuovi sistemi Cloud Volumes ONTAP .
Licenza basata su nodo scaduta acquistata tramite BYOL	Utilizzando questa licenza non avrai diritto a distribuire nuovi sistemi Cloud Volumes ONTAP . I sistemi esistenti potrebbero continuare a funzionare, ma non riceverai alcun supporto o aggiornamento per i tuoi sistemi dopo la data di fine del supporto.
Licenza valida basata su nodi con abbonamento PAYGO	Non riceverai più supporto NetApp dopo la data di fine del supporto, finché non passerai a una licenza basata sulla capacità.

Esclusioni

NetApp riconosce che determinate situazioni richiedono una considerazione speciale e che l'EOA e l'EOS delle licenze basate sui nodi non si applicheranno ai seguenti casi:

- Clienti del settore pubblico statunitense
- Distribuzioni in modalità privata
- Distribuzioni nella regione cinese di Cloud Volumes ONTAP in AWS

Per questi scenari particolari, NetApp offrirà supporto per soddisfare i requisiti di licenza unici nel rispetto degli obblighi contrattuali e delle esigenze operative.

Anche in questi scenari, le nuove licenze basate sui nodi e i rinnovi delle licenze sono validi per un massimo di un anno dalla data di approvazione.

Conversione della licenza

La console consente una conversione senza interruzioni delle licenze basate sui nodi in licenze basate sulla capacità tramite lo strumento di conversione delle licenze. Per informazioni sull'EOA delle licenze basate sui nodi, fare riferimento a"Fine della disponibilità delle licenze basate sui nodi" .

Prima di effettuare la transizione, è bene familiarizzare con la differenza tra i due modelli di licenza. Le licenze basate sui nodi includono una capacità fissa per ogni istanza ONTAP , il che può limitare la flessibilità. Le licenze basate sulla capacità, d'altro canto, consentono di condividere un pool di storage su più istanze, offrendo maggiore flessibilità, ottimizzando l'utilizzo delle risorse e riducendo il rischio di sanzioni finanziarie durante la ridistribuzione dei carichi di lavoro. La ricarica basata sulla capacità si adatta perfettamente alle mutevoli esigenze di stoccaggio.

Per sapere come eseguire questa conversione, fare riferimento a"Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità" .

La conversione di un sistema da una licenza basata sulla capacità a una basata sui nodi non è supportata.

Scopri di più sulle licenze basate sulla capacità per Cloud Volumes ONTAP

È necessario avere familiarità con la tariffazione e l'utilizzo della capacità per le licenze basate sulla capacità.

Modelli di consumo o opzioni di acquisto della licenza

Sono disponibili pacchetti di licenze basati sulla capacità con i seguenti modelli di consumo o opzioni di acquisto:

- **BYOL**: Porta la tua patente (BYOL). Una licenza acquistata da NetApp che può essere utilizzata per distribuire Cloud Volumes ONTAP in qualsiasi provider cloud.

  NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAP" .

- **PAYGO**: Un abbonamento pay-as-you-go (PAYGO) è un abbonamento orario dal marketplace del tuo provider cloud.
- **Annuale**: un contratto annuale dal marketplace del tuo provider cloud.

Notare quanto segue:

- Se acquisti una licenza da NetApp (BYOL), devi anche abbonarti all'offerta PAYGO dal marketplace del tuo provider cloud. NetApp ha limitato le licenze BYOL. Alla scadenza delle licenze BYOL, dovrai sostituirle con abbonamenti al marketplace cloud.

  L'addebito avviene sempre per primo sulla tua licenza, ma nei seguenti casi ti verrà addebitata la tariffa oraria del marketplace:

  - Se superi la capacità autorizzata
  - Se scade il termine della tua licenza
- Se hai un contratto annuale da un marketplace, *tutti* i sistemi Cloud Volumes ONTAP che distribuisci vengono addebitati su quel contratto. Non è possibile combinare un contratto annuale di marketplace con BYOL.
- Solo i sistemi a nodo singolo con BYOL sono supportati nelle regioni della Cina. Le distribuzioni nella regione della Cina sono esenti dalle restrizioni di licenza BYOL.

Modifica dei pacchetti di licenza

Dopo la distribuzione, è possibile modificare il pacchetto per un sistema Cloud Volumes ONTAP che utilizza licenze basate sulla capacità. Ad esempio, se hai distribuito un sistema Cloud Volumes ONTAP con il pacchetto Essentials, puoi modificarlo con il pacchetto Professional se le tue esigenze aziendali cambiano.

"Scopri come cambiare i metodi di ricarica" .

Per informazioni sulla conversione delle licenze basate sui nodi in licenze basate sulla capacità, vedere

Come vengono addebitati i tipi di archiviazione e i pacchetti supportati

La fatturazione in Cloud Volumes ONTAP si basa su una serie di fattori, come pacchetti e tipi di volume. I pacchetti di licenze basati sulla capacità sono disponibili con Cloud Volumes ONTAP 9.7 e versioni successive.

Per i dettagli sui prezzi, vai a "Sito web NetApp Console" .

VM di archiviazione

- Non sono previsti costi di licenza aggiuntivi per le VM di archiviazione dati (SVM) aggiuntive, ma è previsto un costo di capacità minima di 4 TiB per ogni SVM di archiviazione dati.
- Le SVM di disaster recovery vengono fatturate in base alla capacità fornita.

coppie HA

Per le coppie HA, ti verrà addebitata solo la capacità fornita su un nodo. Non ti verrà addebitato alcun costo per i dati che vengono replicati in modo sincrono sul nodo partner.

Volumi FlexClone e FlexCache

- Non ti verrà addebitato alcun costo per la capacità utilizzata dai volumi FlexClone .
- I volumi FlexCache di origine e di destinazione sono considerati dati primari e addebitati in base allo spazio fornito.

Volumi di lettura/scrittura

Se si crea o si utilizza un volume scrivibile (lettura/scrittura), questo viene considerato un volume primario e viene addebitato il costo della capacità fornita in base alla tariffa minima per VM di archiviazione (SVM). Tra gli

esempi rientrano i volumi di lettura/scrittura FlexVol , i volumi di controllo SnapLock e i volumi di controllo CIFS/NFS. Tutti i volumi di dati creati dall'utente vengono addebitati in base al tipo di abbonamento e pacchetto. I volumi interni ONTAP creati automaticamente e che non possono memorizzare dati, come i volumi root SVM, non vengono addebitati.

Pacchetti essenziali

Con il pacchetto Essentials, la fatturazione avviene in base al tipo di distribuzione (HA o nodo singolo) e al tipo di volume (primario o secondario). I prezzi dal più alto al più basso sono nel seguente ordine: *Essentials Primary HA*, *Essentials Primary Single Node*, *Essentials Secondary HA* e *Essentials Secondary Single Node*. In alternativa, quando si acquista un contratto di marketplace o si accetta un'offerta privata, i costi di capacità sono gli stessi per qualsiasi tipo di distribuzione o volume.

La concessione delle licenze si basa interamente sul tipo di volume creato nei sistemi Cloud Volumes ONTAP :

- Nodo singolo Essentials: volumi di lettura/scrittura creati su un sistema Cloud Volumes ONTAP utilizzando un solo nodo ONTAP .
- Essentials HA: volumi di lettura/scrittura che utilizzano due nodi ONTAP che possono eseguire il failover l'uno sull'altro per un accesso ai dati senza interruzioni.
- Nodo singolo secondario Essentials: volumi di tipo Data Protection (DP) (in genere volumi di destinazione SnapMirror o SnapVault di sola lettura) creati su un sistema Cloud Volumes ONTAP utilizzando un solo nodo ONTAP .

  > Se un volume di sola lettura/DP diventa un volume primario, la Console lo considera come dati primari e i costi di addebito vengono calcolati in base al tempo in cui il volume è rimasto in modalità di lettura/scrittura. Quando il volume viene nuovamente reso di sola lettura/DP, il sistema lo considera nuovamente come dati secondari e addebita di conseguenza i costi utilizzando la licenza più adatta nella Console.

- Essentials Secondary HA: volumi di tipo Data Protection (DP) (in genere volumi di destinazione SnapMirror o SnapVault di sola lettura) creati su un sistema Cloud Volumes ONTAP utilizzando due nodi ONTAP che possono eseguire il failover l'uno sull'altro per un accesso ai dati senza interruzioni.

Limite di capacità

Nel modello di licenza basato sulla capacità, ogni sistema Cloud Volumes ONTAP supporta la suddivisione in livelli per l'archiviazione di oggetti e la capacità totale suddivisa in livelli può essere scalata fino al limite del bucket del provider cloud. Sebbene la licenza non imponga restrizioni di capacità, seguire le "Migliori pratiche FabricPool" per garantire prestazioni ottimali, affidabilità ed efficienza dei costi durante la configurazione e la gestione del tiering.

Per informazioni sui limiti di capacità di ciascun provider cloud, fare riferimento alla relativa documentazione:

- "Documentazione AWS"
- "Documentazione di Azure per i dischi gestiti"E "Documentazione di Azure per l'archiviazione BLOB"
- "Documentazione di Google Cloud"

Numero massimo di sistemi

Con le licenze basate sulla capacità, il numero massimo di sistemi Cloud Volumes ONTAP è limitato a 24 per organizzazione della NetApp Console. Un *sistema* è una coppia HA Cloud Volumes ONTAP, un sistema Cloud Volumes ONTAP a nodo singolo o qualsiasi VM di storage aggiuntiva che crei. La VM di storage predefinita non viene conteggiata nel limite. Questo limite si applica a tutti i modelli di licenza.

Ad esempio, supponiamo di avere tre sistemi:

- Un sistema Cloud Volumes ONTAP a nodo singolo con una VM di storage (questa è la VM di storage predefinita creata quando si distribuisce Cloud Volumes ONTAP)

  Questo sistema conta come un unico sistema.

- Un sistema Cloud Volumes ONTAP a nodo singolo con due VM di storage (la VM di storage predefinita, più una VM di storage aggiuntiva creata dall'utente)

  Questo sistema conta come due sistemi: uno per il sistema a nodo singolo e uno per la storage VM aggiuntiva.

- Una coppia Cloud Volumes ONTAP HA con tre VM di storage (la VM di storage predefinita, più due VM di storage aggiuntive create dall'utente)

  Questo sistema conta come tre sistemi: uno per la coppia HA e due per le VM di storage aggiuntive.

In totale sono sei sistemi. A quel punto nella tua organizzazione ci sarebbe spazio per altri 14 sistemi.

Se hai una distribuzione di grandi dimensioni che richiede più di 24 sistemi, contatta il tuo rappresentante commerciale o il team di vendita.

"Scopri i limiti di archiviazione per AWS, Azure e Google Cloud" .

Costo minimo

È previsto un costo minimo di 4 TiB per ogni VM di archiviazione dati che abbia almeno un volume primario (lettura-scrittura). Se la somma dei volumi primari è inferiore a 4 TiB, la Console applica la tariffa minima di 4 TiB a quella VM di archiviazione.

Se non hai ancora effettuato il provisioning di alcun volume, la tariffa minima non verrà applicata.

Per il pacchetto Essentials, la tariffa per la capacità minima di 4 TiB non si applica alle VM di archiviazione che contengono solo volumi secondari (di protezione dei dati). Ad esempio, se si dispone di una VM di archiviazione con 1 TiB di dati secondari, verrà addebitato solo quel 1 TiB di dati. Con il tipo di pacchetto Professional, la capacità minima di ricarica di 4 TiB si applica indipendentemente dal tipo di volume.

Preferenze di fatturazione e superamenti

Puoi scegliere la modalità di addebito nella sezione * Licenses and subscriptions* della Console. Si verificano eccedenze quando l'utilizzo supera la capacità specificata nel pacchetto di licenza o nell'abbonamento annuale.

- * Licenze NetApp prima*: in questo modello, l'utilizzo viene addebitato prima sulla capacità del pacchetto di licenze (BYOL). Se superi la capacità della tua licenza, le eccedenze verranno addebitate in base all'abbonamento annuale al marketplace o alle tariffe orarie on-demand del marketplace (PAYGO). Se la licenza BYOL scade, è necessario passare a un modello di licenza basato sulla capacità tramite i marketplace cloud. Per informazioni, fare riferimento a "Convertire una licenza basata su nodi Cloud Volumes ONTAP in una licenza basata sulla capacità".
- **Solo abbonamenti al Marketplace**: con questo modello, l'utilizzo viene addebitato innanzitutto sull'abbonamento annuale al Marketplace. Ogni utilizzo aggiuntivo verrà addebitato in base alle tariffe orarie on-demand del marketplace (PAYGO). L'eventuale capacità di licenza non utilizzata non viene presa in considerazione ai fini della fatturazione.

Per ulteriori informazioni sulle preferenze di fatturazione, fare riferimento a "Scopri di più sulle preferenze di fatturazione per licenze e abbonamenti".

Come vengono addebitati gli eccessi per le licenze Essentials

Se acquisti una licenza Essentials da NetApp (BYOL) e superi la capacità concessa in licenza per uno specifico pacchetto Essentials, la Console addebita le eccedenze su una licenza Essentials più costosa (se ne hai una con capacità disponibile). La Console utilizza innanzitutto la capacità disponibile per cui hai pagato prima di addebitare l'importo sul marketplace. Se non è disponibile capacità con la tua licenza BYOL, la capacità eccedente verrà addebitata in base alle tariffe orarie on-demand del marketplace (PAYGO) e aggiunta alla tua fattura mensile.

Allo stesso modo, se si dispone di un contratto annuale di marketplace o di un'offerta privata con più pacchetti Essentials e l'utilizzo supera la capacità impegnata per una distribuzione e un tipo di volume di un pacchetto specifico, la Console addebita le eccedenze su un pacchetto Essentials più costoso in base alla sua capacità disponibile. Una volta esaurita tale capacità, l'eccedenza residua viene fatturata secondo le tariffe orarie del marketplace on-demand (PAYGO) e aggiunta alla fattura mensile.

Per informazioni sulla tariffazione delle licenze Essentials, fare riferimento a"Pacchetti essenziali" .

Ecco un esempio. Supponiamo che tu abbia le seguenti licenze per il pacchetto Essentials:

- Una licenza *Essentials Secondary HA* da 500 TiB con capacità impegnata di 500 TiB
- Una licenza *Essentials Single Node* da 500 TiB che ha solo 100 TiB di capacità impegnata

Altri 50 TiB sono forniti su una coppia HA con volumi secondari. Invece di addebitare quei 50 TiB a PAYGO, la Console addebita l'eccedenza di 50 TiB sulla licenza *Essentials Single Node*. Questa licenza ha un prezzo più alto rispetto a *Essentials Secondary HA*, ma utilizza una licenza che hai già acquistato e non aggiungerà costi alla tua fattura mensile.

In **Amministrazione > Licenses and subscriptions**, puoi vedere 50 TiB addebitati sulla licenza *Essentials Single Node*.

Ecco un altro esempio. Supponiamo che tu abbia le seguenti licenze per il pacchetto Essentials:

- Una licenza *Essentials Secondary HA* da 500 TiB con capacità impegnata di 500 TiB
- Una licenza *Essentials Single Node* da 500 TiB che ha solo 100 TiB di capacità impegnata

Altri 100 TiB sono forniti su una coppia HA con volumi primari. La licenza acquistata non dispone della capacità impegnata per *Essentials Primary HA*. La licenza *Essentials Primary HA* ha un prezzo più alto rispetto alle licenze *Essentials Primary Single Node* e *Essentials Secondary HA*.

In questo esempio, la Console addebita le eccedenze alla tariffa di mercato per i 100 TiB aggiuntivi. Gli addebiti per il superamento del limite massimo appariranno sulla tua fattura mensile.

Magazzinaggio

Protocolli client supportati per Cloud Volumes ONTAP

Cloud Volumes ONTAP supporta i protocolli client iSCSI, NFS, SMB, NVMe-TCP e S3.

iSCSI

iSCSI è un protocollo a blocchi che può essere eseguito su reti Ethernet standard. La maggior parte dei sistemi operativi client offre un iniziatore software che funziona tramite una porta Ethernet standard.

NFS

NFS è il protocollo tradizionale di accesso ai file per i sistemi UNIX e LINUX. I client possono accedere ai file nei volumi ONTAP utilizzando i protocolli NFSv3, NFSv4 e NFSv4.1. È possibile controllare l'accesso ai file utilizzando autorizzazioni in stile UNIX, autorizzazioni in stile NTFS o una combinazione di entrambe.

I client possono accedere agli stessi file utilizzando sia i protocolli NFS che SMB.

PMI

SMB è il protocollo tradizionale di accesso ai file per i sistemi Windows. I client possono accedere ai file nei volumi ONTAP utilizzando i protocolli SMB 2.0, SMB 2.1, SMB 3.0 e SMB 3.1.1. Proprio come con NFS, è supportato un mix di stili di autorizzazione.

S3

Cloud Volumes ONTAP supporta S3 come opzione per l'archiviazione scalabile. Il supporto del protocollo S3 consente di configurare l'accesso client S3 agli oggetti contenuti in un bucket in una VM di archiviazione (SVM).

"Documentazione ONTAP : scopri come funziona il multiprotocollo S3" . "Documentazione ONTAP : scopri come configurare e gestire i servizi di archiviazione di oggetti S3 in ONTAP" .

NVMe-TCP

A partire dalla versione 9.12.1 ONTAP , NVMe-TCP è supportato da tutti i provider cloud. Cloud Volumes ONTAP supporta NVMe-TCP come protocollo a blocchi per le VM di archiviazione (SVM) durante la distribuzione e installa automaticamente le licenze NVMe richieste.

NetApp Console non fornisce alcuna funzionalità di gestione per NVMe-TCP.

Per ulteriori informazioni sulla configurazione di NVMe tramite ONTAP, fare riferimento a "Documentazione ONTAP : configurare una VM di archiviazione per NVMe" .

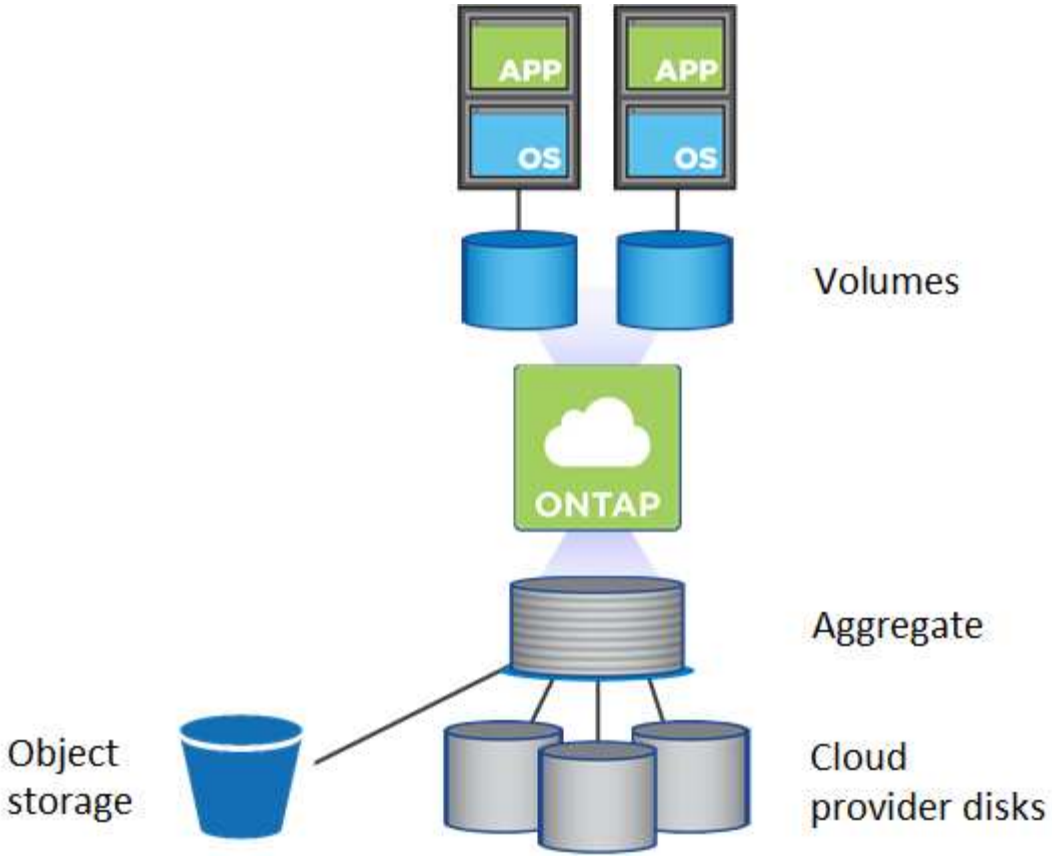
Dischi e aggregati utilizzati per i cluster Cloud Volumes ONTAP

Comprendere come Cloud Volumes ONTAP utilizza l'archiviazione cloud può aiutarti a comprendere i costi di archiviazione.

È necessario creare ed eliminare tutti i dischi e gli aggregati dalla NetApp Console. Non dovresti eseguire queste azioni da un altro strumento di gestione. Ciò potrebbe compromettere la stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare commissioni ridondanti per il provider cloud.

Panoramica

Cloud Volumes ONTAP utilizza lo storage del provider cloud come dischi e li raggruppa in uno o più aggregati. Gli aggregati forniscono spazio di archiviazione a uno o più volumi.



Sono supportati diversi tipi di dischi cloud. Quando si crea un volume, si sceglie il tipo di disco e quando si distribuisce Cloud Volumes ONTAP si seleziona la dimensione predefinita del disco.

La quantità totale di spazio di archiviazione acquistato da un fornitore cloud è la *capacità grezza*. La *capacità utilizzabile* è inferiore perché circa il 12-14 percento è costituito da overhead riservato all'utilizzo Cloud Volumes ONTAP . Ad esempio, se la Console crea un aggregato da 500 GiB, la capacità utilizzabile è 442,94 GiB.

Deposito AWS

In AWS, Cloud Volumes ONTAP utilizza l'archiviazione EBS per i dati utente e l'archiviazione NVMe locale come cache Flash su alcuni tipi di istanze EC2.

Deposito EBS

In AWS, un aggregato può contenere fino a 6 dischi tutti della stessa dimensione. Tuttavia, se si dispone di una configurazione che supporta la funzionalità Amazon EBS Elastic Volumes, un aggregato può contenere fino a 8 dischi. "Scopri di più sul supporto per Elastic Volumes" .

La dimensione massima del disco è 16 TiB.

Il tipo di disco EBS sottostante può essere un SSD per uso generico (gp3 o gp2), un SSD Provisioned IOPS (io1) o un HDD Throughput Optimized (st1). È possibile associare un disco EBS ad Amazon Simple Storage Service (Amazon S3) per "archiviazione di oggetti a basso costo".

Si sconsiglia di suddividere i dati in livelli per l'archiviazione di oggetti quando si utilizzano HDD Throughput Optimized (st1).

Archiviazione NVMe locale

Alcuni tipi di istanza EC2 includono l'archiviazione NVMe locale, che Cloud Volumes ONTAP utilizza come"Cache flash" .

Link correlati

- "Documentazione AWS: Tipi di volume EBS"
- "Scopri come scegliere i tipi e le dimensioni dei dischi per i tuoi sistemi in AWS"
- "Esaminare i limiti di archiviazione per Cloud Volumes ONTAP in AWS"
- "Esamina le configurazioni supportate per Cloud Volumes ONTAP in AWS"

Archiviazione di Azure

In Azure, un aggregato può contenere fino a 12 dischi che sono tutti della stessa dimensione. Il tipo di disco e la dimensione massima del disco dipendono dal fatto che si utilizzi un sistema a nodo singolo o una coppia HA:

Sistemi a nodo singolo

I sistemi a nodo singolo possono utilizzare questi tipi di Azure Managed Disks:

- I dischi gestiti SSD Premium offrono prestazioni elevate per carichi di lavoro ad alta intensità di I/O a un costo più elevato.
- I dischi gestiti Premium SSD v2 offrono prestazioni più elevate con una latenza inferiore a un costo inferiore sia per i singoli nodi che per le coppie HA, rispetto ai dischi gestiti Premium SSD.
- I dischi gestiti SSD standard garantiscono prestazioni costanti per carichi di lavoro che richiedono IOPS bassi.
- I dischi gestiti HDD standard sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

  Ogni tipo di disco gestito ha una dimensione massima del disco di 32 TiB.

  È possibile associare un disco gestito all'archiviazione BLOB di Azure per"archiviazione di oggetti a basso costo" .

coppie HA

Le coppie HA utilizzano due tipi di dischi che garantiscono prestazioni elevate per carichi di lavoro ad alta intensità di I/O a un costo più elevato:

- *Blob di pagina premium* con una dimensione massima del disco di 8 TiB
- *Dischi gestiti* con una dimensione massima del disco di 32 TiB

Link correlati

- "Scopri come scegliere i tipi e le dimensioni dei dischi per i tuoi sistemi in Azure"
- "Avvia una coppia Cloud Volumes ONTAP HA in Azure"
- "Documentazione di Microsoft Azure: tipi di dischi gestiti di Azure"
- "Documentazione di Microsoft Azure: Panoramica dei blob di pagine di Azure"
- "Esaminare i limiti di archiviazione per Cloud Volumes ONTAP in Azure"

Archiviazione Google Cloud

In Google Cloud, un aggregato può contenere fino a 6 dischi tutti della stessa dimensione. La dimensione massima del disco è 64 TiB.

Il tipo di disco può essere *dischi persistenti SSD zonali*, *dischi persistenti bilanciati zonali* o *dischi persistenti standard zonali*. È possibile associare dischi persistenti a un bucket di Google Storage per"archiviazione di oggetti a basso costo" .

Link correlati

- "Documentazione di Google Cloud: Opzioni di archiviazione"
- "Esamina i limiti di archiviazione per Cloud Volumes ONTAP in Google Cloud"

Tipo RAID

Il tipo RAID per ogni aggregato Cloud Volumes ONTAP è RAID0 (striping). Cloud Volumes ONTAP si affida al provider cloud per la disponibilità e la durabilità dei dischi. Non sono supportati altri tipi di RAID.

Ricambi a caldo

RAID0 non supporta l'uso di hot spare per la ridondanza.

La creazione di dischi inutilizzati (hot spare) collegati a un'istanza di Cloud Volumes ONTAP è una spesa non necessaria e potrebbe impedire il provisioning di spazio aggiuntivo secondo necessità. Pertanto non è consigliabile.

Scopri di più sul supporto per AWS Elastic Volumes con Cloud Volumes ONTAP

Il supporto per la funzionalità Amazon EBS Elastic Volumes con un aggregato Cloud Volumes ONTAP garantisce prestazioni migliori e capacità aggiuntiva, consentendo al contempo alla NetApp Console di aumentare automaticamente la capacità del disco sottostante in base alle necessità.

Benefici

- Crescita dinamica del disco

  La console può aumentare dinamicamente le dimensioni dei dischi mentre Cloud Volumes ONTAP è in esecuzione e mentre i dischi sono ancora collegati.

- Prestazioni migliori

  Gli aggregati abilitati con Elastic Volumes possono avere fino a otto dischi utilizzati equamente su due gruppi RAID. Questa configurazione garantisce una maggiore produttività e prestazioni costanti.

- Aggregati più grandi

  Il supporto per otto dischi garantisce una capacità aggregata massima di 128 TiB. Questi limiti sono superiori al limite di sei dischi e al limite di 96 TiB per gli aggregati che non sono abilitati con la funzionalità Elastic Volumes.

  Si noti che i limiti della capacità totale del sistema rimangono invariati.

"Documentazione AWS: Scopri di più su Elastic Volumes di AWS"

Configurazioni supportate

La funzionalità Amazon EBS Elastic Volumes è supportata con specifiche versioni Cloud Volumes ONTAP e specifici tipi di dischi EBS.

Versione Cloud Volumes ONTAP

La funzionalità Elastic Volumes è supportata con i *nuovi* sistemi Cloud Volumes ONTAP creati a partire dalla versione 9.11.0 o successive. La funzionalità *non* è supportata con i sistemi Cloud Volumes ONTAP esistenti distribuiti prima della versione 9.11.0.

Ad esempio, la funzionalità Elastic Volumes non è supportata se hai creato un sistema Cloud Volumes ONTAP 9.9.0 e successivamente hai aggiornato tale sistema alla versione 9.11.0. Deve trattarsi di un nuovo sistema distribuito utilizzando la versione 9.11.0 o successiva.

Tipi di dischi EBS

La funzionalità Elastic Volumes viene abilitata automaticamente a livello aggregato quando si utilizzano SSD per uso generico (gp3) o SSD Provisioned IOPS (io1). La funzionalità Elastic Volumes non è supportata con aggregati che utilizzano altri tipi di disco.

Autorizzazioni AWS richieste

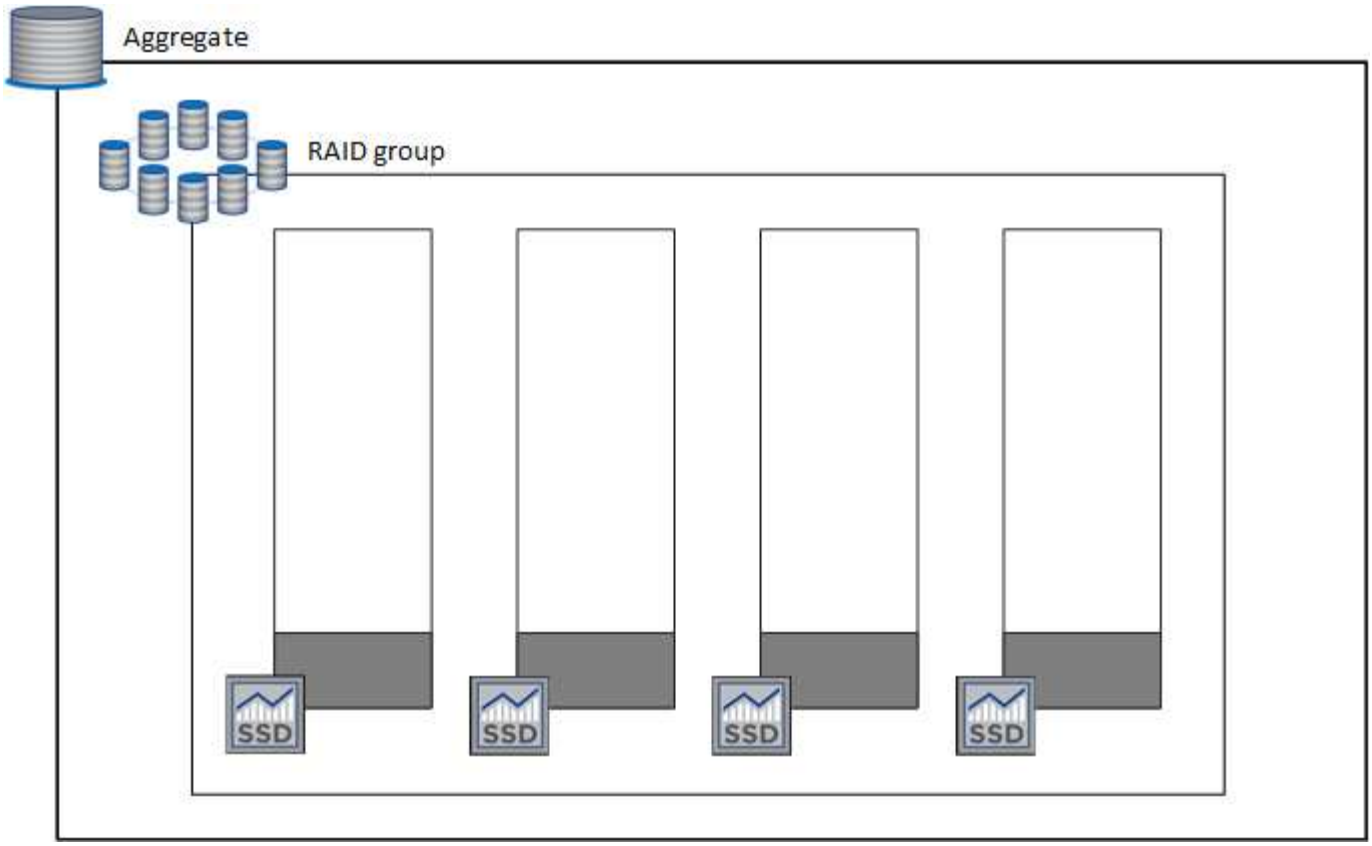
A partire dalla versione 3.9.19, l'agente Console richiede le seguenti autorizzazioni per abilitare e gestire la funzionalità Elastic Volumes su un aggregato Cloud Volumes ONTAP :

- ec2:DescribeVolumesModifications
- ec2:ModificaVolume

Questi permessi sono inclusi in "le policy fornite da NetApp"

Come funziona il supporto per Elastic Volumes

Un aggregato con la funzionalità Elastic Volumes abilitata è composto da uno o due gruppi RAID. Ogni gruppo RAID è composto da quattro dischi identici con la stessa capacità. Ecco un esempio di un aggregato da 10 TiB con quattro dischi da 2,5 TiB ciascuno:



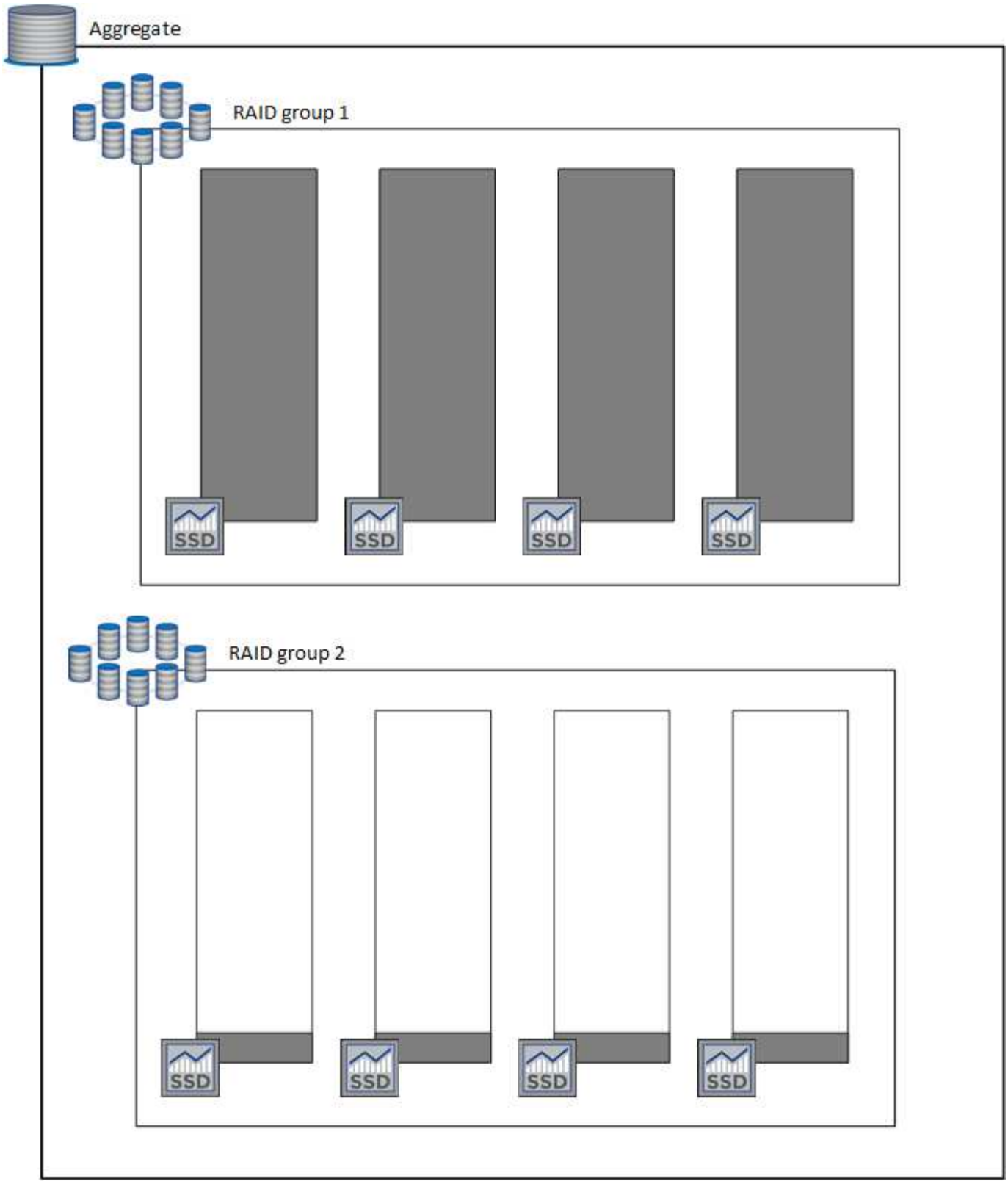
Quando la console crea un aggregato, inizia con un gruppo RAID. Se è necessaria capacità aggiuntiva, l'aggregato aumenta della stessa quantità la capacità di tutti i dischi nel gruppo RAID. L'aumento di capacità è pari ad almeno 256 GiB o al 10% delle dimensioni dell'aggregato.

Ad esempio, se si dispone di un aggregato da 1 TiB, ogni disco è da 250 GiB. Il 10% della capacità dell'aggregato è pari a 100 GiB. Si tratta di una quantità inferiore a 256 GiB, quindi la dimensione dell'aggregato aumenta del minimo di 256 GiB (o 64 GiB per ciascun disco).

La console aumenta le dimensioni dei dischi mentre il sistema Cloud Volumes ONTAP è in esecuzione e mentre i dischi sono ancora collegati. Il cambiamento non è dirompente.

Se un aggregato raggiunge 64 TiB (o 16 TiB su ciascun disco), la Console crea un secondo gruppo RAID per capacità aggiuntiva. Questo secondo gruppo RAID funziona esattamente come il primo: è composto da quattro dischi che hanno esattamente la stessa capacità e possono arrivare fino a 64 TiB. Ciò significa che un aggregato può avere una capacità massima di 128 TiB.

Ecco un esempio di aggregazione con due gruppi RAID. È stato raggiunto il limite di capacità sul primo gruppo RAID, mentre i dischi del secondo gruppo RAID dispongono di molto spazio libero.



Cosa succede quando si crea un volume

Se si crea un volume che utilizza dischi gp3 o io1, la Console crea il volume su un aggregato come segue:

- Se è presente un aggregato gp3 o io1 esistente con Elastic Volumes abilitato, la Console crea il volume su tale aggregato.

- Se sono presenti più aggregati gp3 o io1 con Elastic Volumes abilitato, la Console crea il volume sull'aggregato che richiede la quantità minima di risorse.
- Se il sistema dispone solo di aggregati gp3 o io1 non abilitati per Elastic Volumes, il volume viene creato su tale aggregato.

> Sebbene questo scenario sia improbabile, è possibile in due casi:
>
> - Hai disabilitato esplicitamente la funzionalità Elastic Volumes durante la creazione di un aggregato dall'API.
> - Hai creato un nuovo sistema Cloud Volumes ONTAP dall'interfaccia utente, nel qual caso la funzionalità Elastic Volumes è disabilitata nell'aggregato iniziale. RevisioneLimitazioni qui sotto per saperne di più.

- Se nessun aggregato esistente ha capacità sufficiente, la Console crea l'aggregato con Elastic Volumes abilitato e quindi crea il volume su quel nuovo aggregato.

  La dimensione dell'aggregato si basa sul volume richiesto più un ulteriore 10% di capacità.

Modalità di gestione della capacità

La modalità di gestione della capacità per un agente della console funziona con Elastic Volumes in modo simile a come funziona con altri tipi di aggregati:

- Quando è abilitata la modalità Automatica (impostazione predefinita), la Console aumenta automaticamente le dimensioni degli aggregati se è necessaria capacità aggiuntiva.
- Se si modifica la modalità di gestione della capacità in Manuale, la Console chiederà la tua approvazione per acquistare capacità aggiuntiva.

"Scopri di più sulla modalità di gestione della capacità" .

Limitazioni

L'aumento delle dimensioni di un aggregato può richiedere fino a 6 ore. Durante tale periodo, la Console non può richiedere alcuna capacità aggiuntiva per tale aggregato.

Come lavorare con i volumi elastici

Con Elastic Volumes puoi eseguire queste attività:

- Crea un nuovo sistema con Elastic Volumes abilitato sull'aggregato iniziale quando si utilizzano dischi gp3 o io1

  "Scopri come creare il sistema Cloud Volumes ONTAP"

- Crea un nuovo volume su un aggregato in cui sono abilitati i volumi elastici

  Se si crea un volume che utilizza dischi gp3 o io1, la Console crea automaticamente il volume su un aggregato in cui Elastic Volumes è abilitato. Per maggiori dettagli, fare riferimento aCosa succede quando si crea un volume .

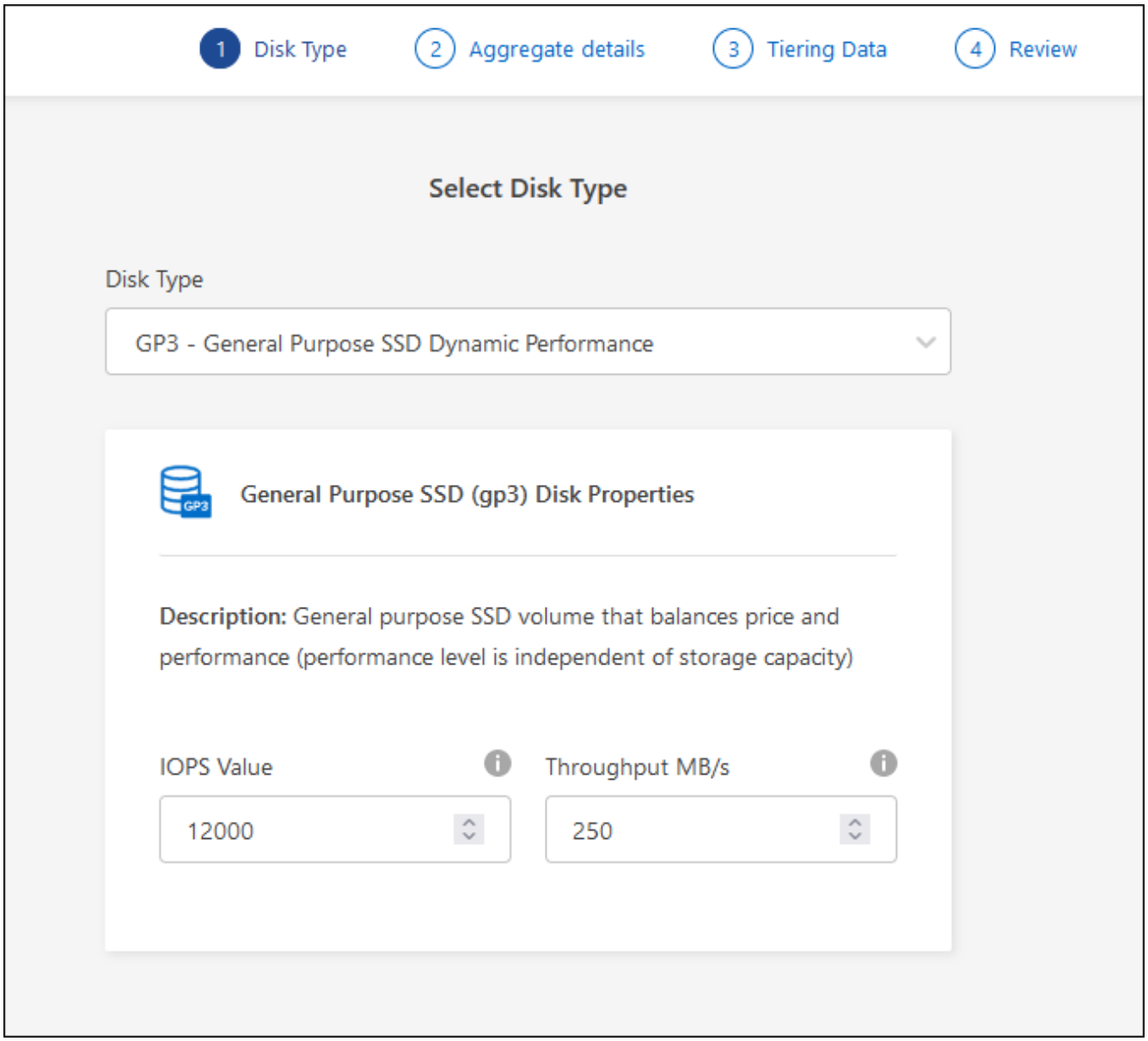
  "Impara a creare volumi" .

- Crea un nuovo aggregato con Elastic Volumes abilitato

Elastic Volumes viene abilitato automaticamente sui nuovi aggregati che utilizzano dischi gp3 o io1, a condizione che il sistema Cloud Volumes ONTAP sia stato creato a partire dalla versione 9.11.0 o successiva.

Quando si crea l'aggregato, la Console richiede di specificare la dimensione della capacità dell'aggregato. Questa configurazione è diversa da altre in cui si sceglie la dimensione del disco e il numero di dischi.

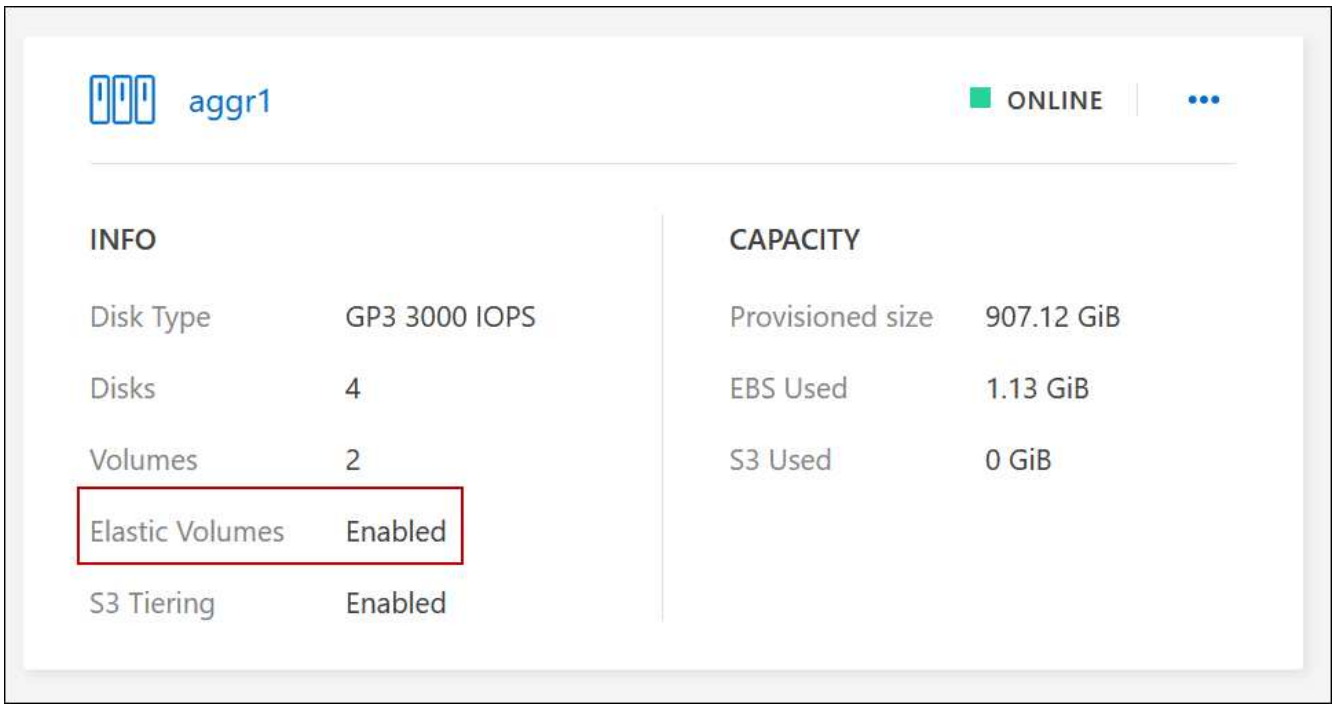
La seguente schermata mostra un esempio di un nuovo aggregato composto da dischi gp3.



"Scopri come creare aggregati" .

- Identifica gli aggregati che hanno Elastic Volumes abilitato

Quando si accede alla pagina Allocazione avanzata, è possibile verificare se la funzionalità Elastic Volumes è abilitata su un aggregato. Nell'esempio seguente, aggr1 ha Elastic Volumes abilitato.



- Aggiungere capacità a un aggregato

  Sebbene la Console aggiunga automaticamente capacità agli aggregati in base alle necessità, è possibile aumentare manualmente la capacità.

  "Scopri come aumentare la capacità aggregata" .

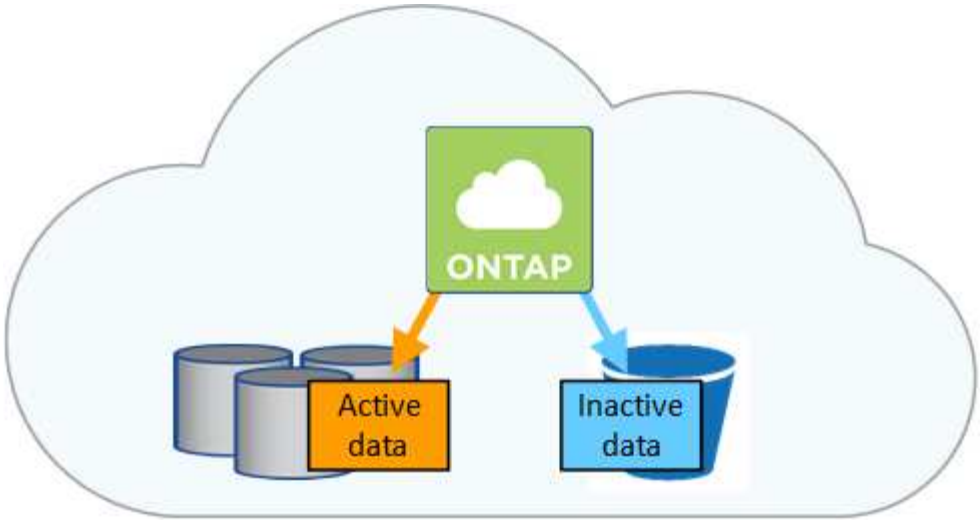
- Replicare i dati in un aggregato con Elastic Volumes abilitato

  Se il sistema Cloud Volumes ONTAP di destinazione supporta Elastic Volumes, un volume di destinazione verrà posizionato su un aggregato in cui Elastic Volumes è abilitato (a condizione che si scelga un disco gp3 o io1).

  "Scopri come impostare la replica dei dati"

Scopri di più sulla suddivisione in livelli dei dati con Cloud Volumes ONTAP in AWS, Azure o Google Cloud

Riduci i costi di archiviazione abilitando la suddivisione automatica dei dati inattivi in un archivio di oggetti a basso costo. I dati attivi rimangono negli SSD o HDD ad alte prestazioni, mentre i dati inattivi vengono archiviati in sistemi di archiviazione a oggetti a basso costo. Ciò consente di recuperare spazio sullo storage primario e di ridurre lo storage secondario.



La suddivisione in livelli dei dati è basata sulla tecnologia FabricPool . Cloud Volumes ONTAP fornisce livelli di dati per tutti i cluster Cloud Volumes ONTAP senza una licenza aggiuntiva. Quando si abilita il data tiering, i dati suddivisi in livelli per l'archiviazione degli oggetti comportano dei costi. Per maggiori dettagli sui costi di archiviazione degli oggetti, consulta la documentazione del tuo provider cloud.

Livelli di dati in AWS

Quando si abilita il data tiering in AWS, Cloud Volumes ONTAP utilizza EBS come livello di prestazioni per i dati hot e Amazon Simple Storage Service (Amazon S3) come livello di capacità per i dati inattivi.

Livello di prestazione

Il livello di prestazioni può essere costituito da SSD per uso generico (gp3 o gp2) o SSD Provisioned IOPS (io1).

Si sconsiglia di suddividere i dati in livelli per l'archiviazione di oggetti quando si utilizzano HDD Throughput Optimized (st1).

Livello di capacità

Un sistema Cloud Volumes ONTAP suddivide i dati inattivi in un singolo bucket S3.

La NetApp Console crea un singolo bucket S3 per ciascun sistema e lo denomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket S3 diverso per ogni volume.

Quando la Console crea il bucket S3, utilizza le seguenti impostazioni predefinite:

- Classe di stoccaggio: Standard
- Crittografia predefinita: disabilitata
- Blocca l'accesso pubblico: blocca tutto l'accesso pubblico
- Proprietà dell'oggetto: ACL abilitati
- Versionamento del bucket: disabilitato
- Blocco oggetto: disabilitato

Classi di archiviazione

La classe di archiviazione predefinita per i dati a livelli in AWS è *Standard*. Standard è ideale per i dati a cui si accede frequentemente e che sono archiviati in più zone di disponibilità.

Se non si prevede di accedere ai dati inattivi, è possibile ridurre i costi di archiviazione modificando la classe di archiviazione in una delle seguenti: *Intelligent Tiering*, *One-Zone Infrequent Access*, *Standard-Infrequent Access* o *S3 Glacier Instant Retrieval*. Quando si modifica la classe di archiviazione, i dati inattivi iniziano nella classe di archiviazione Standard e passano alla classe di archiviazione selezionata, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi è opportuno tenerne conto prima di modificare la classe di archiviazione. "Documentazione di Amazon S3: Scopri di più sulle classi di archiviazione di Amazon S3" .

È possibile selezionare una classe di archiviazione quando si crea il sistema e modificarla in qualsiasi momento successivo. Per istruzioni sulla modifica della classe di archiviazione, fare riferimento a"Suddividi i dati inattivi in un archivio di oggetti a basso costo" .

La classe di archiviazione per la suddivisione in livelli dei dati è a livello di sistema e non per volume.

Livelli dei dati in Azure

Quando si abilita la suddivisione in livelli dei dati in Azure, Cloud Volumes ONTAP utilizza i dischi gestiti di Azure come livello di prestazioni per i dati attivi e l'archiviazione BLOB di Azure come livello di capacità per i dati inattivi.

Livello di prestazione

Il livello di prestazioni può essere costituito da SSD o HDD.

Livello di capacità

Un sistema Cloud Volumes ONTAP suddivide i dati inattivi in livelli in un singolo contenitore BLOB.

La console crea un nuovo account di archiviazione con un contenitore per ogni sistema Cloud Volumes ONTAP . Il nome dell'account di archiviazione è casuale. Non viene creato un contenitore diverso per ogni volume.

La console crea l'account di archiviazione con le seguenti impostazioni:

- Livello di accesso: Caldo
- Prestazioni: Standard
- Ridondanza: in base alla distribuzione di Cloud Volume ONTAP
  - Zona di disponibilità singola: archiviazione ridondante locale (LRS)
  - Zona di disponibilità multipla: archiviazione con ridondanza di zona (ZRS)
- Account: StorageV2 (uso generale v2)
- Richiedi trasferimento sicuro per le operazioni API REST: abilitato
- Accesso alla chiave dell'account di archiviazione: abilitato
- Versione TLS minima: versione 1.2
- Crittografia dell'infrastruttura: disabilitata

Livelli di accesso all'archiviazione

Il livello di accesso all'archiviazione predefinito per i dati a livelli in Azure è il livello *hot*. Il livello caldo è ideale per i dati a cui si accede frequentemente nel livello di capacità.

Se non si prevede di accedere ai dati inattivi nel livello di capacità, è possibile scegliere il livello di

archiviazione *cool*, in cui i dati inattivi vengono conservati per un minimo di 30 giorni. È anche possibile optare per il livello *cold*, in cui i dati inattivi vengono archiviati per un minimo di 90 giorni. In base alle tue esigenze di archiviazione e alle considerazioni sui costi, puoi selezionare il livello più adatto alle tue esigenze. Quando si modifica il livello di archiviazione in *cool* o *cold*, i dati del livello di capacità inattivo vengono spostati direttamente nel livello di archiviazione cool o cold. I livelli cool e cold offrono costi di archiviazione inferiori rispetto al livello hot, ma comportano costi di accesso più elevati, quindi tienilo in considerazione prima di cambiare livello di archiviazione. Fare riferimento a "Documentazione di Microsoft Azure: Scopri di più sui livelli di accesso all'archiviazione BLOB di Azure" .

È possibile selezionare un livello di archiviazione quando si aggiunge un sistema Cloud Volumes ONTAP e modificarlo in qualsiasi momento successivo. Per i dettagli sulla modifica del livello di archiviazione, fare riferimento a"Suddividi i dati inattivi in un archivio di oggetti a basso costo" .

Il livello di accesso all'archiviazione per la suddivisione in livelli dei dati è a livello di sistema e non per volume.

Livelli dei dati in Google Cloud

Quando si abilita la suddivisione in livelli dei dati in Google Cloud, Cloud Volumes ONTAP utilizza dischi persistenti come livello di prestazioni per i dati attivi e un bucket Google Cloud Storage come livello di capacità per i dati inattivi.

Livello di prestazione

Il livello di prestazioni può essere costituito da dischi persistenti SSD, dischi persistenti bilanciati o dischi persistenti standard.

Livello di capacità

Un sistema Cloud Volumes ONTAP suddivide i dati inattivi in un singolo bucket di Google Cloud Storage.

La console crea un bucket per ciascun sistema e lo denomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket diverso per ogni volume.

Quando la Console crea il bucket, utilizza le seguenti impostazioni predefinite:

- Tipo di posizione: Regione
- Classe di stoccaggio: Standard
- Accesso pubblico: soggetto agli ACL degli oggetti
- Controllo degli accessi: a grana fine
- Protezione: Nessuna
- Crittografia dei dati: chiave gestita da Google

Classi di archiviazione

La classe di archiviazione predefinita per i dati a livelli è la classe *Standard Storage*. Se l'accesso ai dati avviene raramente, è possibile ridurre i costi di archiviazione passando a *Nearline Storage* o *Coldline Storage*. Quando si modifica la classe di archiviazione, i dati inattivi successivi vengono spostati direttamente nella classe selezionata.

> Tutti i dati inattivi esistenti manterranno la classe di archiviazione predefinita quando si modifica la classe di archiviazione. Per modificare la classe di archiviazione per i dati inattivi esistenti, è necessario eseguire la designazione manualmente.

I costi di accesso sono più elevati se si accede ai dati, quindi è opportuno tenerne conto prima di modificare

la classe di archiviazione. Per saperne di più, fare riferimento al "Documentazione di Google Cloud: Classi di archiviazione" .

È possibile selezionare un livello di archiviazione quando si crea il sistema e modificarlo in qualsiasi momento successivo. Per i dettagli sulla modifica della classe di archiviazione, fare riferimento a"Suddividi i dati inattivi in un archivio di oggetti a basso costo" .

La classe di archiviazione per la suddivisione in livelli dei dati è a livello di sistema e non per volume.

Livelli di dati e limiti di capacità

Se si abilita la suddivisione in livelli dei dati, il limite di capacità del sistema rimane invariato. Il limite è suddiviso tra il livello di prestazioni e il livello di capacità.

Criteri di suddivisione in livelli del volume

Per abilitare la suddivisione in livelli dei dati, è necessario selezionare un criterio di suddivisione in livelli del volume quando si crea, si modifica o si replica un volume. È possibile selezionare una policy diversa per ogni volume.

Alcune policy di suddivisione in livelli prevedono un periodo di raffreddamento minimo associato, che stabilisce il tempo per cui i dati utente in un volume devono rimanere inattivi affinché vengano considerati "freddi" e spostati nel livello di capacità. Il periodo di raffreddamento inizia quando i dati vengono scritti nell'aggregato.

È possibile modificare il periodo minimo di raffreddamento e la soglia aggregata predefinita del 50% (maggiori dettagli di seguito). "Scopri come modificare il periodo di raffreddamento" E "impara come cambiare la soglia" .

La Console consente di scegliere tra i seguenti criteri di suddivisione in livelli del volume quando si crea o si modifica un volume:

Solo istantanea

Dopo che un aggregato ha raggiunto il 50% della capacità, Cloud Volumes ONTAP suddivide i dati utente inattivi delle copie Snapshot non associate al file system attivo nel livello di capacità. Il periodo di raffreddamento è di circa 2 giorni.

Se letti, i blocchi di dati freddi sul livello di capacità diventano caldi e vengono spostati sul livello di prestazioni.

Tutto

Tutti i dati (esclusi i metadati) vengono immediatamente contrassegnati come cold e trasferiti nell'archiviazione degli oggetti il prima possibile. Non è necessario attendere 48 ore affinché i nuovi blocchi di un volume si raffreddino. Si noti che i blocchi presenti nel volume prima dell'impostazione del criterio All richiedono 48 ore per raffreddarsi.

Se letti, i blocchi di dati freddi sul livello cloud restano freddi e non vengono riscritti sul livello delle prestazioni. Questa policy è disponibile a partire da ONTAP 9.6.

Auto

Dopo che un aggregato ha raggiunto il 50% della capacità, Cloud Volumes ONTAP suddivide i blocchi di dati freddi in un volume in un livello di capacità. I dati freddi includono non solo le copie Snapshot, ma anche i dati utente freddi provenienti dal file system attivo. Il periodo di raffreddamento è di circa 31 giorni.

Questa policy è supportata a partire da Cloud Volumes ONTAP 9.4.

Se letti tramite letture casuali, i blocchi di dati freddi nel livello di capacità diventano caldi e passano al livello di prestazioni. Se letti tramite letture sequenziali, come quelle associate alle scansioni di indici e antivirus, i blocchi di dati freddi rimangono freddi e non passano al livello di prestazioni.

Nessuno

Mantiene i dati di un volume nel livello delle prestazioni, impedendone lo spostamento nel livello della capacità.

Replicazione

Quando si replica un volume, è possibile scegliere se suddividere i dati in livelli di archiviazione degli oggetti. In tal caso, la Console applica il criterio **Backup** al volume di protezione dei dati. A partire da Cloud Volumes ONTAP 9.6, la policy di tiering **All** sostituisce la policy di backup. Quando una relazione di replicazione viene eliminata, il volume di destinazione mantiene la politica di suddivisione in livelli in vigore durante la replicazione.

La disattivazione di Cloud Volumes ONTAP influisce sul periodo di raffreddamento

I blocchi di dati vengono raffreddati tramite scansioni di raffreddamento. Durante questo processo, la temperatura dei blocchi non utilizzati viene spostata (raffreddata) al valore immediatamente inferiore. Il tempo di raffreddamento predefinito dipende dalla politica di suddivisione in livelli del volume:

- Auto: 31 giorni
- Solo snapshot: 2 giorni

Per far funzionare la scansione di raffreddamento, è necessario che Cloud Volumes ONTAP sia in esecuzione. Se Cloud Volumes ONTAP è disattivato, anche il raffreddamento verrà interrotto. Di conseguenza, è possibile ottenere tempi di raffreddamento più lunghi.

Quando Cloud Volumes ONTAP è disattivato, la temperatura di ciascun blocco viene mantenuta fino al riavvio del sistema. Ad esempio, se la temperatura di un blocco è 5 quando si spegne il sistema, la temperatura sarà ancora 5 quando si riaccende il sistema.

Impostazione della suddivisione in livelli dei dati

Per istruzioni e un elenco delle configurazioni supportate, fare riferimento a"Suddividi i dati inattivi in un archivio di oggetti a basso costo" .

Gestione dello storage Cloud Volumes ONTAP

La NetApp Console offre una gestione semplificata e avanzata dello storage Cloud Volumes ONTAP .

È necessario creare ed eliminare tutti i dischi e gli aggregati direttamente dalla Console. Non dovresti eseguire queste azioni da un altro strumento di gestione. Ciò potrebbe compromettere la stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare commissioni ridondanti per il provider cloud.

Provisioning dello storage

La Console semplifica il provisioning dello storage per Cloud Volumes ONTAP acquistando dischi e gestendo gli aggregati per te. Devi solo creare volumi. Se lo desideri, puoi utilizzare un'opzione di allocazione avanzata per effettuare autonomamente il provisioning degli aggregati.

Provisioning semplificato

Gli aggregati forniscono spazio di archiviazione cloud ai volumi. La console crea aggregati per te quando avvii un'istanza e quando esegui il provisioning di volumi aggiuntivi.

Quando si crea un volume, la Console esegue una delle tre operazioni seguenti:

- Colloca il volume su un aggregato esistente che dispone di spazio libero sufficiente.
- Colloca il volume su un aggregato esistente acquistando più dischi per quell'aggregato.

+ Nel caso di un aggregato in AWS che supporta Elastic Volumes, aumenta anche la dimensione dei dischi in un gruppo RAID. "Scopri di più sul supporto per Elastic Volumes" .

- Acquista dischi per un nuovo aggregato e posiziona il volume su quell'aggregato.

La console determina dove posizionare un nuovo volume prendendo in considerazione diversi fattori: la dimensione massima di un aggregato, se il thin provisioning è abilitato e le soglie di spazio libero per gli aggregati.

Selezione delle dimensioni del disco per gli aggregati in AWS

Quando la Console crea nuovi aggregati per Cloud Volumes ONTAP in AWS, aumenta gradualmente le dimensioni del disco man mano che aumentano i numeri degli aggregati per massimizzare la capacità del sistema prima di raggiungere i limiti dei dischi dati AWS.

Ad esempio, la Console potrebbe scegliere le seguenti dimensioni del disco:

Numero aggregato	Dimensione del disco	Capacità massima aggregata
1	500 GB	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB

Questo comportamento non si applica agli aggregati che supportano la funzionalità Amazon EBS Elastic Volumes. Gli aggregati in cui è abilitato Elastic Volumes sono composti da uno o due gruppi RAID. Ogni gruppo RAID è composto da quattro dischi identici con la stessa capacità. "Scopri di più sul supporto per Elastic Volumes" .

È possibile scegliere autonomamente la dimensione del disco utilizzando l'opzione di allocazione avanzata.

Assegnazione anticipata

È anche possibile gestire gli aggregati. "Dalla pagina **Assegnazione avanzata**" , è possibile creare nuovi aggregati che includono un numero specifico di dischi, aggiungere dischi a un aggregato esistente e creare volumi in aggregati specifici.

Gestione della capacità

L'amministratore dell'organizzazione o dell'account può configurare la Console in modo che ti informi sulle decisioni relative alla capacità di archiviazione o che gestisca automaticamente i requisiti di capacità per te.

Questo comportamento è determinato dalla *Modalità di gestione della capacità* su un agente della console. La modalità di gestione della capacità interessa tutti i sistemi Cloud Volumes ONTAP gestiti da quell'agente della

console. Se si dispone di un altro agente Console, è possibile configurarlo in modo diverso.

Gestione automatica della capacità

Per impostazione predefinita, la modalità di gestione della capacità è impostata su automatica. In questa modalità, la console controlla il rapporto di spazio libero ogni 15 minuti per determinare se tale rapporto scende al di sotto della soglia specificata. Se è necessaria maggiore capacità, avvia l'acquisto di nuovi dischi, elimina le raccolte di dischi non utilizzate (aggregati), sposta i volumi tra gli aggregati secondo necessità e tenta di impedire guasti ai dischi.

Gli esempi seguenti illustrano il funzionamento di questa modalità:

- Se un aggregato raggiunge la soglia di capacità e ha spazio per altri dischi, la Console acquista automaticamente nuovi dischi per quell'aggregato, in modo che i volumi possano continuare a crescere.

Nel caso di un aggregato in AWS che supporta Elastic Volumes, aumenta anche la dimensione dei dischi in un gruppo RAID. "Scopri di più sul supporto per Elastic Volumes" .

+ * Se un aggregato raggiunge la soglia di capacità e non può supportare dischi aggiuntivi, la Console sposta automaticamente un volume da quell'aggregato a un aggregato con capacità disponibile o a un nuovo aggregato.

+ Se la Console crea un nuovo aggregato per il volume, sceglie una dimensione del disco che si adatti alla dimensione di quel volume.

+ Si noti che ora è disponibile spazio libero sull'aggregato originale. Tale spazio può essere utilizzato sia da volumi esistenti che da nuovi volumi. In questo scenario lo spazio non può essere restituito al provider cloud.

- Se un aggregato non contiene volumi per più di 12 ore, la Console lo elimina.

Gestione delle LUN con gestione automatica della capacità

La gestione automatica della capacità della Console non si applica alle LUN. Quando crea un LUN, disabilita la funzionalità di aumento automatico.

Gestione manuale della capacità

Se l'amministratore dell'organizzazione o dell'account imposta la **Modalità di gestione della capacità** su manuale, la Console ti informa di intraprendere le azioni appropriate per le decisioni sulla capacità. Gli stessi esempi descritti nella modalità automatica si applicano alla modalità manuale, ma spetta a te accettare le azioni.

Saperne di più

"Scopri come modificare la modalità di gestione della capacità" .

velocità di scrittura

NetApp Console consente di scegliere una velocità di scrittura normale o elevata per la maggior parte delle configurazioni Cloud Volumes ONTAP . Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normale e alta, nonché i rischi e i consigli relativi all'utilizzo di una velocità di scrittura elevata.

Velocità di scrittura normale

Quando si sceglie la velocità di scrittura normale, i dati vengono scritti direttamente sul disco. Quando i dati vengono scritti direttamente su disco, si riduce la probabilità di perdita di dati in caso di interruzione imprevista del sistema o di un guasto a cascata che comporta un'interruzione imprevista del sistema (solo coppie HA).

L'opzione predefinita è la velocità di scrittura normale.

Alta velocità di scrittura

Quando si sceglie un'elevata velocità di scrittura, i dati vengono memorizzati in un buffer nella memoria prima di essere scritti sul disco, il che garantisce prestazioni di scrittura più rapide. A causa di questa memorizzazione nella cache, esiste il rischio di perdita di dati in caso di interruzione imprevista del sistema.

La quantità di dati che può andare persa in caso di interruzione imprevista del sistema è pari all'intervallo degli ultimi due punti di coerenza. Un punto di coerenza è l'atto di scrivere dati memorizzati nel buffer su disco. Un punto di coerenza si verifica quando il registro di scrittura è pieno o dopo 10 secondi (a seconda di quale evento si verifica per primo). Tuttavia, le prestazioni dello storage fornito dal tuo provider cloud possono influire sul tempo di elaborazione del punto di coerenza.

Quando utilizzare un'elevata velocità di scrittura

Un'elevata velocità di scrittura è una buona scelta se sono richieste prestazioni di scrittura rapide per il carico di lavoro e si può resistere al rischio di perdita di dati in caso di interruzione imprevista del sistema o di un guasto a cascata che comporta un'interruzione imprevista del sistema (solo coppie HA).

Raccomandazioni per l'utilizzo di velocità di scrittura elevate

Se si abilita un'elevata velocità di scrittura, è necessario garantire la protezione da scrittura a livello di applicazione o che le applicazioni siano in grado di tollerare la perdita di dati, qualora si verifichi.

Elevata velocità di scrittura con una coppia HA in AWS

Se si prevede di abilitare un'elevata velocità di scrittura su una coppia HA in AWS, è necessario comprendere la differenza nei livelli di protezione tra una distribuzione con più zone di disponibilità (AZ) e una distribuzione con una sola AZ. L'implementazione di una coppia HA su più AZ garantisce maggiore resilienza e può contribuire a ridurre il rischio di perdita di dati.

"Scopri di più sulle coppie HA in AWS" .

Configurazioni che supportano un'elevata velocità di scrittura

Non tutte le configurazioni Cloud Volumes ONTAP supportano velocità di scrittura elevate. Per impostazione predefinita, queste configurazioni utilizzano la velocità di scrittura normale.

AWS

Se si utilizza un sistema a nodo singolo, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con tutti i tipi di istanza.

A partire dalla versione 9.8, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con coppie HA quando si utilizzano quasi tutti i tipi di istanze EC2 supportati, ad eccezione di m5.xlarge e r5.xlarge.

"Scopri di più sulle istanze Amazon EC2 supportate da Cloud Volumes ONTAP" .

Azzurro

Se si utilizza un sistema a nodo singolo, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con tutti i tipi di istanze di macchine virtuali.

Se si utilizza una coppia HA, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con diversi tipi di VM, a partire dalla versione 9.8. Vai al "Note sulla versione Cloud Volumes ONTAP" per visualizzare i tipi di VM che supportano un'elevata velocità di scrittura.

Google Cloud

Se si utilizza un sistema a nodo singolo, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con tutti i tipi di macchine.

Se si utilizza una coppia HA, Cloud Volumes ONTAP supporta un'elevata velocità di scrittura con diversi tipi di VM, a partire dalla versione 9.13.0. Vai al "Note sulla versione Cloud Volumes ONTAP" per visualizzare i tipi di VM che supportano un'elevata velocità di scrittura.

"Scopri di più sui tipi di macchine Google Cloud supportati da Cloud Volumes ONTAP" .

Come selezionare una velocità di scrittura

È possibile scegliere una velocità di scrittura quando si aggiunge un nuovo sistema Cloud Volumes ONTAP e si può"modificare la velocità di scrittura per un sistema esistente" .

Cosa aspettarsi in caso di perdita di dati

Se si verifica una perdita di dati a causa dell'elevata velocità di scrittura, l'Event Management System (EMS) segnala i due eventi seguenti:

- Cloud Volumes ONTAP 9.12.1 o versione successiva

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP da 9.11.0 a 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP da 9.8 a 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

Quando ciò accade, Cloud Volumes ONTAP dovrebbe essere in grado di avviarsi e continuare a fornire dati senza l'intervento dell'utente.

Come interrompere l'accesso ai dati in caso di perdita di dati

Se si teme la perdita di dati e si desidera che le applicazioni smettano di funzionare in caso di perdita di dati e che l'accesso ai dati venga ripreso dopo aver risolto correttamente il problema della perdita di dati, è possibile utilizzare l'opzione NVFAIL dalla CLI per raggiungere tale obiettivo.

Per abilitare l'opzione NVFAIL

```
vol modify -volume <vol-name> -nvfail on
```

Per controllare le impostazioni NVFAIL

```
vol show -volume <vol-name> -fields nvfail
```

Per disabilitare l'opzione NVFAIL

```
vol modify -volume <vol-name> -nvfail off
```

Quando si verifica una perdita di dati, un volume NFS o iSCSI con NVFAIL abilitato dovrebbe smettere di fornire dati (non vi è alcun impatto su CIFS, che è un protocollo stateless). Per maggiori dettagli, fare riferimento a "In che modo NVFAIL influisce sull'accesso ai volumi NFS o LUN" .

Per controllare lo stato NVFAIL

```
vol show -fields in-nvfailed-state
```

Dopo aver risolto correttamente il problema della perdita di dati, è possibile cancellare lo stato NVFAIL e il volume sarà disponibile per l'accesso ai dati.

Per cancellare lo stato NVFAIL

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Cache flash

Alcune configurazioni Cloud Volumes ONTAP includono storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash Cache* per prestazioni migliori.

Cos'è Flash Cache?

Flash Cache velocizza l'accesso ai dati tramite la memorizzazione nella cache intelligente in tempo reale dei dati utente letti di recente e dei metadati NetApp . È efficace per carichi di lavoro ad alta intensità di lettura casuale, tra cui database, posta elettronica e servizi di file.

Configurazioni supportate

Flash Cache è supportato con configurazioni specifiche Cloud Volumes ONTAP . Visualizza le configurazioni supportate in "Note sulla versione Cloud Volumes ONTAP"

Limitazioni

- Quando si configura Flash Cache per Cloud Volumes ONTAP 9.12.0 o versioni precedenti in AWS, la compressione deve essere disabilitata su tutti i volumi per sfruttare i miglioramenti delle prestazioni di Flash Cache. Quando si esegue la distribuzione o l'aggiornamento a Cloud Volumes ONTAP 9.12.1 o versioni successive, non è necessario disabilitare la compressione.

  Salta la selezione delle impostazioni di efficienza di archiviazione quando crei un volume dalla NetApp Console oppure crea un volume e poi "disabilitare la compressione dei dati utilizzando la CLI" .

- Il riscaldamento della cache dopo un riavvio non è supportato con Cloud Volumes ONTAP.

Argomenti correlati

- "Configurazioni supportate per Cloud Volumes ONTAP in AWS"
- "Configurazioni supportate per Cloud Volumes ONTAP in Azure"
- "Configurazioni supportate per Cloud Volumes ONTAP in Google Cloud"

Scopri di più sullo storage WORM su Cloud Volumes ONTAP

È possibile attivare l'archiviazione WORM (Write Once, Read Many) su un sistema Cloud Volumes ONTAP per conservare i file in formato non modificato per un periodo di conservazione specificato. L'archiviazione Cloud WORM è basata sulla tecnologia SnapLock , il che significa che i file WORM sono protetti a livello di file.

La funzionalità WORM è disponibile per l'uso con la licenza BYOL (Bring Your Own License) e gli abbonamenti al marketplace per le tue licenze senza costi aggiuntivi. Contatta il tuo rappresentante commerciale NetApp per aggiungere WORM alla tua licenza attuale.

Come funziona l'archiviazione WORM

Una volta che un file è stato memorizzato nell'archivio WORM, non può essere modificato, nemmeno dopo la scadenza del periodo di conservazione. Un orologio a prova di manomissione determina quando è trascorso il periodo di conservazione di un file WORM.

Una volta trascorso il periodo di conservazione, sarai responsabile dell'eliminazione di tutti i file di cui non hai più bisogno.

Attivazione dell'archiviazione WORM

La modalità di attivazione dell'archiviazione WORM dipende dalla versione Cloud Volumes ONTAP utilizzata.

Versione 9.10.1 e successive

A partire da Cloud Volumes ONTAP 9.10.1, è possibile abilitare o disabilitare WORM a livello di volume.

Quando si aggiunge un sistema Cloud Volumes ONTAP , viene richiesto di abilitare o disabilitare l'archiviazione WORM:

- Se si abilita l'archiviazione WORM quando si aggiunge un sistema, ogni volume creato dalla NetApp Console avrà WORM abilitato. Ma è possibile utilizzare ONTAP System Manager o ONTAP CLI per creare volumi con WORM disabilitato.
- Se si disabilita l'archiviazione WORM quando si aggiunge un sistema, in ogni volume creato dalla Console,

da ONTAP System Manager o da ONTAP CLI la funzionalità WORM sarà disabilitata.

Versione 9.10.0 e precedenti

È possibile attivare l'archiviazione WORM su un sistema Cloud Volumes ONTAP quando si aggiunge un nuovo sistema. Ogni volume creato dalla Console ha WORM abilitato. Non è possibile disattivare l'archiviazione WORM su singoli volumi.

Commit di file su WORM

È possibile utilizzare un'applicazione per eseguire il commit dei file in WORM tramite NFS o CIFS oppure utilizzare ONTAP CLI per eseguire automaticamente il commit dei file in WORM. È anche possibile utilizzare un file WORM aggiungibile per conservare i dati scritti in modo incrementale, come le informazioni di registro.

Dopo aver attivato l'archiviazione WORM su un sistema Cloud Volumes ONTAP , è necessario utilizzare l'interfaccia a riga di comando ONTAP per tutta la gestione dell'archiviazione WORM. Per le istruzioni, fare riferimento al "Documentazione ONTAP su SnapLock" .

Abilitazione di WORM su un sistema Cloud Volumes ONTAP

È possibile abilitare l'archiviazione WORM durante la creazione di un sistema Cloud Volumes ONTAP sulla Console. È anche possibile abilitare WORM su un sistema se WORM non è abilitato su di esso durante la creazione. Dopo averlo abilitato, non sarà più possibile disabilitare WORM.

Informazioni su questo compito

- WORM è supportato su ONTAP 9.10.1 e versioni successive.
- WORM con backup è supportato su ONTAP 9.11.1 e versioni successive.

Passi

1. Nella pagina **Sistemi**, fare doppio clic sul nome del sistema su cui si desidera abilitare WORM.
2. Nella scheda Panoramica, fare clic sul pannello Funzionalità e quindi sull'icona della matita accanto a **WORM**.

   Se WORM è già abilitato sul sistema, l'icona della matita è disabilitata.

3. Nella pagina **WORM**, impostare il periodo di conservazione per il Compliance Clock del cluster.

   Per maggiori informazioni, fare riferimento al "Documentazione ONTAP : inizializzazione del Compliance Clock" .

4. Fare clic su **Imposta**.

Dopo aver finito

È possibile verificare lo stato di **WORM** nel pannello Funzionalità. Dopo l'abilitazione di WORM, la licenza SnapLock viene installata automaticamente sul cluster. È possibile visualizzare la licenza SnapLock su ONTAP System Manager.

Eliminazione dei file WORM

È possibile eliminare i file WORM durante il periodo di conservazione utilizzando la funzionalità di eliminazione privilegiata.

Per le istruzioni, fare riferimento al "Documentazione ONTAP" .

WORM e livelli di dati

Quando si crea un nuovo sistema Cloud Volumes ONTAP 9.8 o versione successiva, è possibile abilitare contemporaneamente sia il tiering dei dati sia l'archiviazione WORM. Abilitando la suddivisione in livelli dei dati con l'archiviazione WORM è possibile suddividere i dati in livelli in un archivio oggetti nel cloud.

È necessario comprendere quanto segue sull'abilitazione sia del tiering dei dati sia dell'archiviazione WORM:

- I dati suddivisi in livelli per l'archiviazione di oggetti non includono la funzionalità ONTAP WORM. Per garantire la funzionalità WORM end-to-end, è necessario impostare correttamente le autorizzazioni del bucket.
- I dati suddivisi in livelli per l'archiviazione di oggetti non supportano la funzionalità WORM, il che significa che tecnicamente chiunque abbia accesso completo a bucket e contenitori può eliminare gli oggetti suddivisi in livelli da ONTAP.
- Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 è bloccato dopo l'abilitazione di WORM e del tiering.

Limitazioni

- L'archiviazione WORM in Cloud Volumes ONTAP funziona secondo un modello di "amministratore di archiviazione attendibile". Sebbene i file WORM siano protetti da alterazioni o modifiche, i volumi possono essere eliminati da un amministratore del cluster anche se contengono dati WORM non scaduti.
- Oltre al modello di amministratore di storage attendibile, lo storage WORM in Cloud Volumes ONTAP opera implicitamente anche secondo un modello di "amministratore cloud attendibile". Un amministratore cloud potrebbe eliminare i dati WORM prima della loro scadenza rimuovendo o modificando l'archiviazione cloud direttamente dal provider cloud.

Link correlato

- "Crea copie Snapshot a prova di manomissione per l'archiviazione WORM"
- "Licenze e addebiti in Cloud Volumes ONTAP"

Coppie ad alta disponibilità

Scopri di più sulle coppie Cloud Volumes ONTAP HA in AWS

Una configurazione ad alta disponibilità (HA) Cloud Volumes ONTAP garantisce operazioni senza interruzioni e tolleranza agli errori. In AWS, i dati vengono replicati in modo sincrono tra i due nodi.

Componenti HA

In AWS, le configurazioni Cloud Volumes ONTAP HA includono i seguenti componenti:

- Due nodi Cloud Volumes ONTAP i cui dati vengono replicati in modo sincrono tra loro.
- Un'istanza di mediazione che fornisce un canale di comunicazione tra i nodi per agevolare i processi di acquisizione e restituzione dello storage.

Mediatore

Ecco alcuni dettagli chiave sull'istanza del mediatore in AWS:

Tipo di istanza

t3-micro

Dischi

Due dischi st1 da 8 GiB e 4 GiB

Sistema operativo

Debian 11

> Per Cloud Volumes ONTAP 9.10.0 e versioni precedenti, Debian 10 è stato installato sul mediatore.

Aggiornamenti

Quando si aggiorna Cloud Volumes ONTAP, la NetApp Console aggiorna anche l'istanza del mediatore in base alle necessità.

Accesso all'istanza

Quando si crea una coppia Cloud Volumes ONTAP HA dalla Console, viene richiesto di fornire una coppia di chiavi per l'istanza del mediatore. È possibile utilizzare quella coppia di chiavi per l'accesso SSH utilizzando `admin` utente.

Agenti terzi

Gli agenti di terze parti o le estensioni VM non sono supportati sull'istanza del mediatore.

Acquisizione e restituzione dello spazio di archiviazione

Se un nodo si interrompe, l'altro nodo può fornire dati al suo partner per garantire la continuità del servizio dati. I client possono accedere agli stessi dati dal nodo partner perché i dati sono stati replicati in modo sincrono sul partner.

Dopo il riavvio del nodo, il partner deve risincronizzare i dati prima di poter restituire l'archiviazione. Il tempo necessario per risincronizzare i dati dipende dalla quantità di dati modificati mentre il nodo era inattivo.

L'acquisizione, la risincronizzazione e la restituzione dello storage sono tutte operazioni automatiche per impostazione predefinita. Non è richiesta alcuna azione da parte dell'utente.

RPO e RTO

Una configurazione HA mantiene l'elevata disponibilità dei dati come segue:

- L'obiettivo del punto di ripristino (RPO) è 0 secondi. I tuoi dati sono coerenti a livello transazionale e non subiscono perdite.
- L'obiettivo del tempo di recupero (RTO) è di 120 secondi. In caso di interruzione, i dati dovrebbero essere disponibili entro 120 secondi o meno.

Modelli di distribuzione HA

È possibile garantire l'elevata disponibilità dei dati distribuendo una configurazione HA su più zone di disponibilità (AZ) o in una singola zona di disponibilità (AZ). Dovresti esaminare più nel dettaglio ogni configurazione per scegliere quella più adatta alle tue esigenze.

Zone di disponibilità multiple

L'implementazione di una configurazione HA in più zone di disponibilità (AZ) garantisce un'elevata disponibilità dei dati in caso di errore in una AZ o in un'istanza che esegue un nodo Cloud Volumes ONTAP . È necessario comprendere in che modo gli indirizzi IP NAS influiscono sull'accesso ai dati e sul failover dell'archiviazione.

Accesso ai dati NFS e CIFS

Quando una configurazione HA è distribuita su più zone di disponibilità, gli *indirizzi IP mobili* consentono l'accesso del client NAS. Gli indirizzi IP mobili, che devono trovarsi al di fuori dei blocchi CIDR per tutte le VPC nella regione, possono migrare tra i nodi quando si verificano errori. Non sono accessibili in modo nativo ai client che si trovano al di fuori della VPC, a meno che tu non"configurare un gateway di transito AWS" .

Se non è possibile configurare un gateway di transito, sono disponibili indirizzi IP privati per i client NAS esterni alla VPC. Tuttavia, questi indirizzi IP sono statici e non possono essere sottoposti a failover tra nodi.

Prima di distribuire una configurazione HA su più zone di disponibilità, è opportuno esaminare i requisiti per gli indirizzi IP mobili e le tabelle di routing. Quando si distribuisce la configurazione, è necessario specificare gli indirizzi IP mobili. Gli indirizzi IP privati vengono creati automaticamente.

Per ulteriori informazioni, fare riferimento a "Requisiti di rete AWS per Cloud Volumes ONTAP HA in più AZ" .

Accesso ai dati iSCSI

La comunicazione dati tra VPC non rappresenta un problema poiché iSCSI non utilizza indirizzi IP mobili.

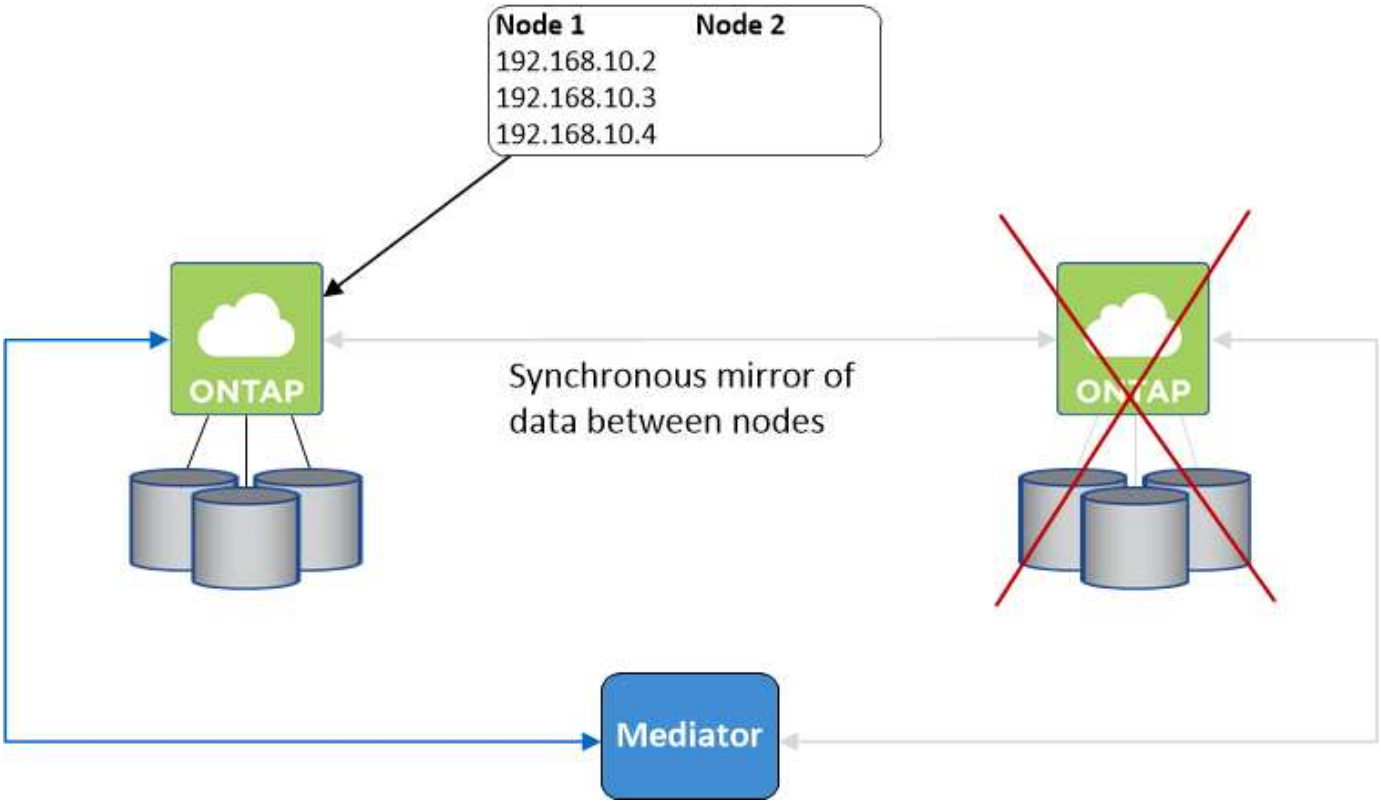
Acquisizione e restituzione per iSCSI

Per iSCSI, Cloud Volumes ONTAP utilizza Multipath I/O (MPIO) e Asymmetric Logical Unit Access (ALUA) per gestire il failover del percorso tra i percorsi ottimizzati attivi e quelli non ottimizzati.

> Per informazioni sulle configurazioni host specifiche che supportano ALUA, fare riferimento a "Strumento matrice di interoperabilità NetApp" e il "Guida agli host SAN e ai client cloud" per il sistema operativo host.

Acquisizione e restituzione per NAS

Quando si verifica un'acquisizione in una configurazione NAS che utilizza IP flottanti, l'indirizzo IP flottante del nodo utilizzato dai client per accedere ai dati viene spostato sull'altro nodo. L'immagine seguente illustra l'acquisizione dello storage in una configurazione NAS utilizzando IP flottanti. Se il nodo 2 non funziona, l'indirizzo IP mobile per il nodo 2 viene spostato al nodo 1.



Gli IP dei dati NAS utilizzati per l'accesso VPC esterno non possono migrare tra i nodi in caso di guasti. Se un nodo va offline, è necessario rimontare manualmente i volumi sui client esterni alla VPC utilizzando l'indirizzo IP sull'altro nodo.

Dopo che il nodo guasto torna online, rimonta i client sui volumi utilizzando l'indirizzo IP originale. Questo passaggio è necessario per evitare il trasferimento di dati non necessari tra due nodi HA, che può avere un impatto significativo sulle prestazioni e sulla stabilità.

È possibile individuare l'indirizzo IP corretto dalla Console selezionando il volume e facendo clic su **Comando di montaggio**.

Zona di disponibilità unica

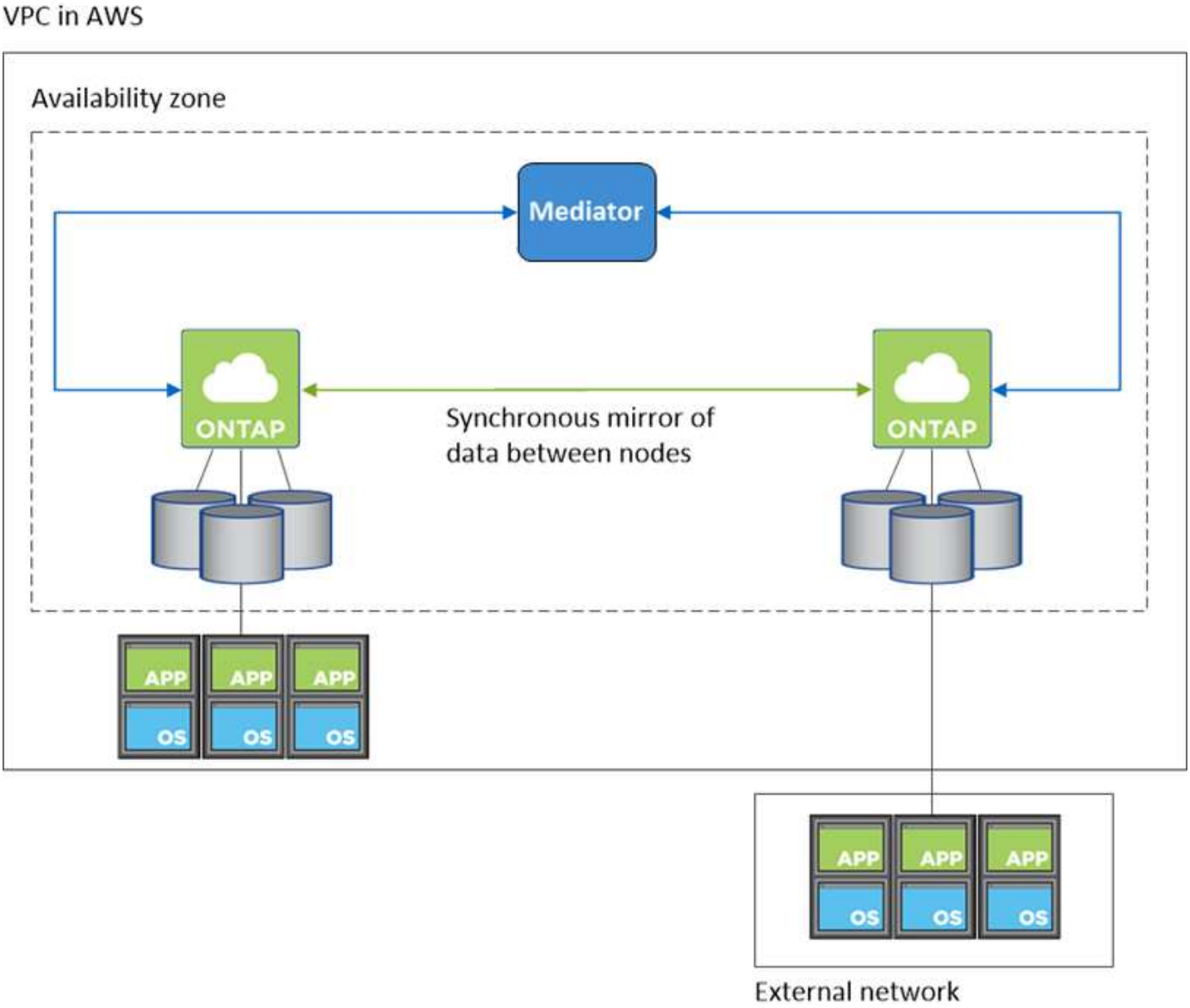
L'implementazione di una configurazione HA in una singola zona di disponibilità (AZ) può garantire un'elevata disponibilità dei dati in caso di errore di un'istanza che esegue un nodo Cloud Volumes ONTAP . Tutti i dati sono accessibili in modo nativo dall'esterno della VPC.

> La console crea un "Documentazione AWS: gruppo di posizionamento diffuso AWS" e avvia i due nodi HA in quel gruppo di posizionamento. Il gruppo di posizionamento riduce il rischio di guasti simultanei distribuendo le istanze su hardware sottostanti distinti. Questa funzionalità migliora la ridondanza dal punto di vista del calcolo e non da quello dei guasti del disco.

Accesso ai dati

Poiché questa configurazione si trova in una singola AZ, non richiede indirizzi IP mobili. È possibile utilizzare lo stesso indirizzo IP per l'accesso ai dati dall'interno e dall'esterno della VPC.

L'immagine seguente mostra una configurazione HA in una singola AZ. I dati sono accessibili sia dall'interno che dall'esterno della VPC.



Acquisizione e restituzione

Per iSCSI, Cloud Volumes ONTAP utilizza Multipath I/O (MPIO) e Asymmetric Logical Unit Access (ALUA) per gestire il failover del percorso tra i percorsi ottimizzati attivi e quelli non ottimizzati.

> Per informazioni sulle configurazioni host specifiche che supportano ALUA, fare riferimento a "Strumento matrice di interoperabilità NetApp" e il "Guida agli host SAN e ai client cloud" per il sistema operativo host.

Per le configurazioni NAS, gli indirizzi IP dei dati possono migrare tra i nodi HA in caso di guasti. Ciò garantisce l'accesso del cliente allo storage.

Zone locali AWS

Le zone locali AWS sono un'implementazione dell'infrastruttura in cui storage, elaborazione, database e altri servizi AWS selezionati sono ubicati in prossimità di grandi città e aree industriali. Con AWS Local Zones puoi avvicinare i servizi AWS a te, migliorando la latenza dei tuoi carichi di lavoro e gestendo i database in locale. Su Cloud Volumes ONTAP,

È possibile distribuire una configurazione AZ singola o AZ multipla nelle zone locali AWS.

Le zone locali AWS sono supportate quando si utilizza la console in modalità standard e privata. Al momento, le zone locali AWS non sono supportate in modalità limitata.

Esempi di configurazioni della zona locale AWS

Cloud Volumes ONTAP in AWS supporta solo la modalità ad alta disponibilità (HA) in una singola zona di disponibilità. Le distribuzioni a nodo singolo non sono supportate.

Cloud Volumes ONTAP non supporta il tiering dei dati, il tiering del cloud e le istanze non qualificate nelle zone locali AWS.

Di seguito sono riportati alcuni esempi di configurazioni:

- Zona di disponibilità singola: sia i nodi del cluster che il mediatore si trovano nella stessa zona locale.
- Zone di disponibilità multiple Nelle configurazioni con zone di disponibilità multiple, sono presenti tre istanze, due nodi e un mediatore. Una delle tre istanze deve trovarsi in una zona separata. Puoi scegliere come impostarlo.

  Ecco tre esempi di configurazioni:

  - Ogni nodo del cluster si trova in una zona locale diversa e il mediatore si trova in una zona di disponibilità pubblica.
  - Un nodo del cluster si trova in una zona locale, il mediatore in una zona locale e il secondo nodo del cluster si trova in una zona di disponibilità.
  - Ogni nodo del cluster e il mediatore si trovano in zone locali separate.

Tipi di dischi e istanze supportati

L'unico tipo di disco supportato è GP2. Attualmente sono supportate le seguenti famiglie di tipi di istanze EC2 con dimensioni da xlarge a 4xlarge:

- M5
- C5
- C5d
- R5
- R5d

Cloud Volumes ONTAP supporta solo queste configurazioni. La selezione di tipi di disco non supportati o di istanze non qualificate nella configurazione AWS Local Zone potrebbe causare errori di distribuzione. Il tiering dei dati su Amazon Simple Storage Service (Amazon S3) non è supportato se il tuo sistema Cloud Volumes ONTAP si trova in una AWS Local Zone, perché l'accesso ai bucket Amazon S3 al di fuori della Local Zone comporta una latenza maggiore e influisce sulle attività di Cloud Volumes ONTAP.

"Documentazione AWS: Tipi di istanza EC2 nelle zone locali" .

Come funziona l’archiviazione in una coppia HA

A differenza di un cluster ONTAP , lo storage in una coppia Cloud Volumes ONTAP HA non è condiviso tra i nodi. Al contrario, i dati vengono replicati in modo sincrono tra i nodi, in modo che siano disponibili anche in caso di guasto.

Assegnazione dello spazio di archiviazione

Quando si crea un nuovo volume e sono necessari dischi aggiuntivi, la Console alloca lo stesso numero di dischi a entrambi i nodi, crea un aggregato con mirroring e quindi crea il nuovo volume. Ad esempio, se per il volume sono necessari due dischi, la Console alloca due dischi per nodo, per un totale di quattro dischi.

Configurazioni di archiviazione

È possibile utilizzare una coppia HA come configurazione attiva-attiva, in cui entrambi i nodi forniscono dati ai client, oppure come configurazione attiva-passiva, in cui il nodo passivo risponde alle richieste di dati solo se ha preso in carico lo storage per il nodo attivo.

È possibile impostare una configurazione attiva-attiva solo quando si utilizza la Console nella Visualizzazione sistema di archiviazione.

Aspettative di prestazione

Una configurazione Cloud Volumes ONTAP HA replica in modo sincrono i dati tra i nodi, consumando larghezza di banda della rete. Di conseguenza, è possibile aspettarsi le seguenti prestazioni rispetto a una configurazione Cloud Volumes ONTAP a nodo singolo:

- Per le configurazioni HA che gestiscono dati da un solo nodo, le prestazioni di lettura sono paragonabili a quelle di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono inferiori.
- Per le configurazioni HA che gestiscono dati da entrambi i nodi, le prestazioni di lettura sono superiori rispetto a quelle di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono uguali o superiori.

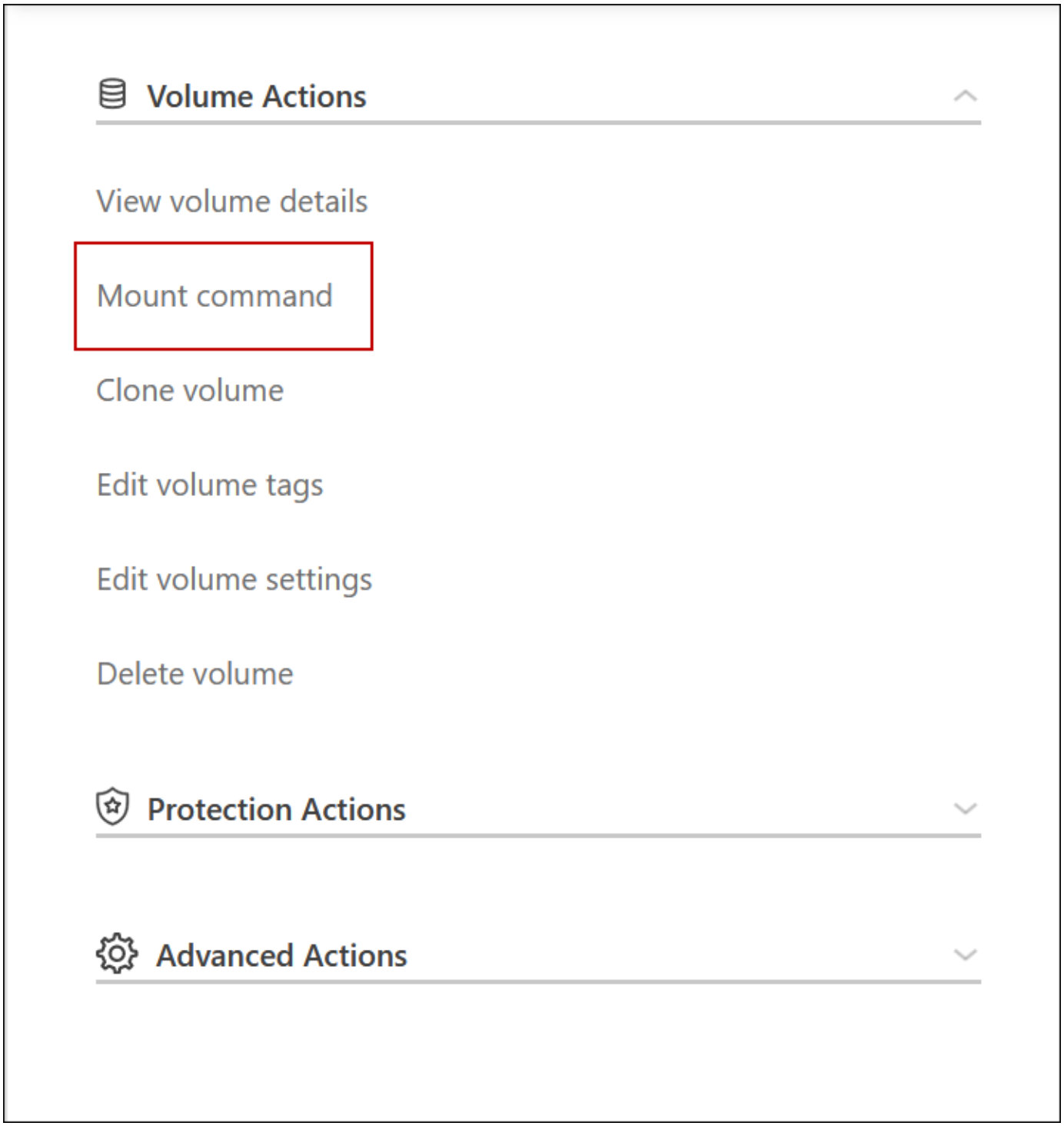
Per maggiori dettagli sulle prestazioni Cloud Volumes ONTAP , fare riferimento a"Prestazione" .

Accesso del cliente allo storage

I client devono accedere ai volumi NFS e CIFS utilizzando l’indirizzo IP dei dati del nodo su cui risiede il volume. Se i client NAS accedono a un volume utilizzando l’indirizzo IP del nodo partner, il traffico viene trasmesso tra entrambi i nodi, riducendo le prestazioni.

Se si sposta un volume tra nodi in una coppia HA, è necessario rimontare il volume utilizzando l’indirizzo IP dell’altro nodo. In caso contrario, le prestazioni potrebbero risultare ridotte. Se i client supportano i riferimenti NFSv4 o il reindirizzamento delle cartelle per CIFS, è possibile abilitare tali funzionalità sui sistemi Cloud Volumes ONTAP per evitare di dover rimontare il volume. Per maggiori dettagli, consultare la documentazione ONTAP .

È possibile identificare facilmente l’indirizzo IP corretto tramite l’opzione *Mount Command* nel pannello di gestione dei volumi.



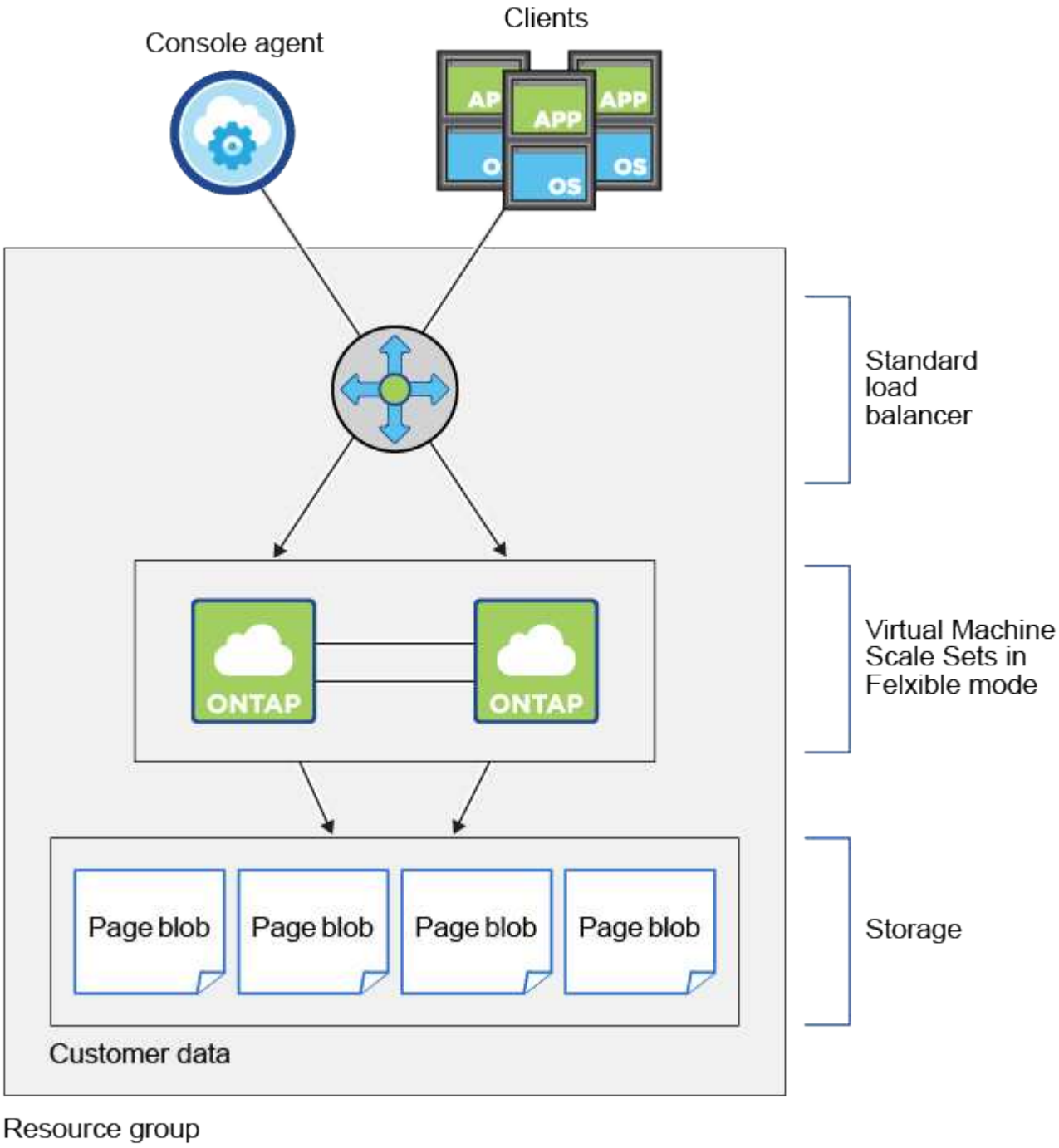
Scopri di più sulle coppie Cloud Volumes ONTAP HA in Azure

Una coppia ad alta disponibilità (HA) Cloud Volumes ONTAP garantisce affidabilità aziendale e continuità operativa in caso di guasti nell'ambiente cloud. In Azure, lo storage è condiviso tra i due nodi.

Componenti HA

Configurazione della zona di disponibilità singola HA con blob di pagina

Una configurazione del blob di pagine HA di Cloud Volumes ONTAP in Azure include i seguenti componenti:



Tieni presente quanto segue sui componenti di Azure che NetApp Console distribuisce per te:

Azure Standard Load Balancer

Il bilanciatore del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP HA.

VM in singole zone di disponibilità

A partire da Cloud Volumes ONTAP 9.15.1, è possibile creare e gestire macchine virtuali (VM) eterogenee in un'unica zona di disponibilità (AZ). È possibile distribuire nodi ad alta disponibilità (HA) in domini di errore

separati all'interno della stessa AZ, garantendo una disponibilità ottimale. Per saperne di più sulla modalità di orchestrazione flessibile che abilita questa capacità, fare riferimento a "Documentazione di Microsoft Azure: set di scalabilità di macchine virtuali" .

Dischi

I dati dei clienti risiedono nei blob delle pagine Premium Storage. Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre necessario ulteriore spazio di archiviazione per"dati di avvio, root e core" .

Account di archiviazione

- Per i dischi gestiti è necessario un account di archiviazione.
- Sono necessari uno o più account di archiviazione per i blob di pagine di archiviazione Premium, poiché è stato raggiunto il limite di capacità del disco per account di archiviazione.

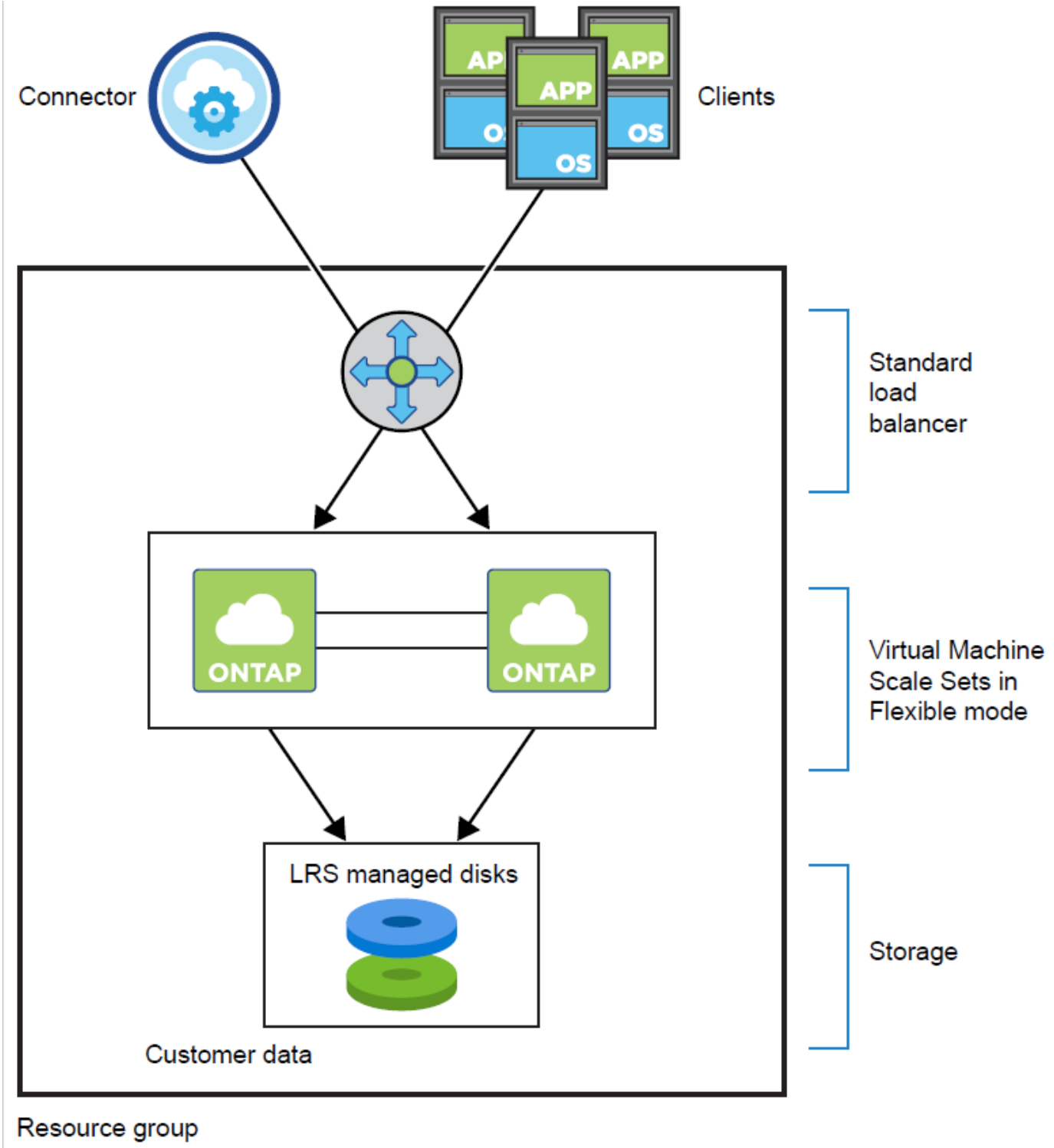
  "Documentazione di Microsoft Azure: obiettivi di scalabilità e prestazioni di Azure Storage per gli account di archiviazione" .

- Per la suddivisione in livelli dei dati nell'archiviazione BLOB di Azure è necessario un account di archiviazione.
- A partire da Cloud Volumes ONTAP 9.7, gli account di archiviazione creati dalla Console per le coppie HA sono account di archiviazione v2 generici.
- È possibile abilitare una connessione HTTPS da una coppia Cloud Volumes ONTAP 9.7 HA agli account di archiviazione di Azure quando si aggiunge un sistema Cloud Volumes ONTAP . Tieni presente che l'abilitazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato il sistema.

> A partire da Cloud Volumes ONTAP 9.15.0P1, i BLOB di pagine di Azure non sono più supportati per le nuove distribuzioni di coppie ad alta disponibilità. Se attualmente si utilizzano BLOB di pagine di Azure in distribuzioni di coppie ad alta disponibilità esistenti, è possibile eseguire la migrazione a tipi di istanze di VM più recenti nelle VM della serie Edsv4 e nelle VM della serie Edsv5. "Scopri di più sulle configurazioni supportate in Azure" .

Configurazione della zona di disponibilità singola HA con dischi gestiti condivisi

Una configurazione di zona di disponibilità singola Cloud Volumes ONTAP HA eseguita su un disco gestito condiviso include i seguenti componenti:



Tieni presente quanto segue sui componenti di Azure che la console distribuisce per te:

Azure Standard Load Balancer

Il bilanciatore del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP HA.

VM in singole zone di disponibilità

A partire da Cloud Volumes ONTAP 9.15.1, è possibile creare e gestire macchine virtuali (VM) eterogenee in un'unica zona di disponibilità (AZ). È possibile distribuire nodi ad alta disponibilità (HA) in domini di errore separati all'interno della stessa AZ, garantendo una disponibilità ottimale. Per saperne di più sulla modalità di orchestrazione flessibile che abilita questa capacità, fare riferimento a "Documentazione di Microsoft

Azure: set di scalabilità di macchine virtuali" .

La distribuzione zonale utilizza Premium SSD v2 Managed Disks quando sono soddisfatte le seguenti condizioni:

- La versione di Cloud Volumes ONTAP è 9.15.1 o successiva.
- La regione e la zona selezionate supportano i dischi gestiti Premium SSD v2. Per informazioni sulle regioni supportate, fare riferimento a "Sito Web di Microsoft Azure: prodotti disponibili per regione" .
- L'abbonamento è registrato per Microsoft"Funzionalità Microsoft.Compute/VMOrchestratorZonalMultiFD" .

Se si sceglie Premium SSD Managed Disks per un ambiente che soddisfa i criteri sopra indicati, la Console distribuisce automaticamente Premium SSD v2 Managed Disks. Non è possibile passare ai dischi gestiti Premium SSD v1.

Dischi

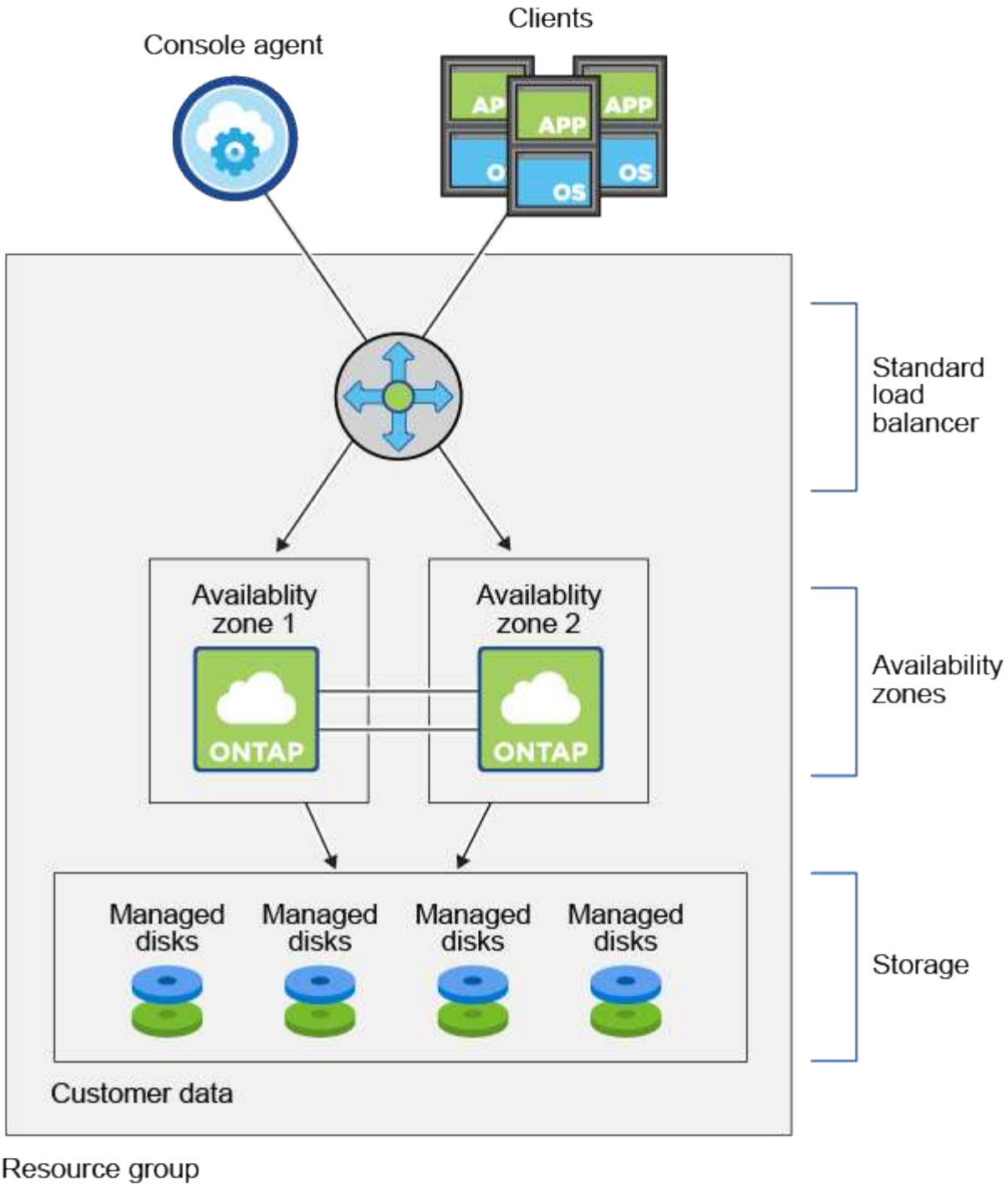
I dati dei clienti risiedono su dischi gestiti con archiviazione ridondante locale (LRS). Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre necessario ulteriore spazio di archiviazione per"dati di avvio, root, root partner, core e NVRAM" .

Account di archiviazione

Gli account di archiviazione vengono utilizzati per le distribuzioni basate su dischi gestiti per gestire i log diagnostici e la suddivisione in livelli nell'archiviazione BLOB.

Configurazione di più zone di disponibilità HA

Una configurazione di più zone di disponibilità HA di Cloud Volumes ONTAP in Azure include i seguenti componenti:



Tieni presente quanto segue sui componenti di Azure che la console distribuisce per te:

Azure Standard Load Balancer

Il bilanciatore del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP HA.

Zone di disponibilità

La configurazione HA con più zone di disponibilità utilizza un modello di distribuzione in cui due nodi Cloud Volumes ONTAP vengono distribuiti in diverse zone di disponibilità, garantendo che i nodi si trovino in domini di errore diversi per garantire ridondanza e disponibilità. Per informazioni su come i set di scalabilità di macchine virtuali in modalità di orchestrazione flessibile possono utilizzare le zone di disponibilità in Azure, fare riferimento a "Documentazione di Microsoft Azure: creare un set di scalabilità di macchine

virtuali che utilizza zone di disponibilità" .

Dischi

I dati dei clienti risiedono su dischi gestiti con archiviazione ridondante di zona (ZRS). Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre necessario ulteriore spazio di archiviazione per"dati di avvio, root, root partner e core" .

Account di archiviazione

Gli account di archiviazione vengono utilizzati per le distribuzioni basate su dischi gestiti per gestire i log diagnostici e la suddivisione in livelli nell'archiviazione BLOB.

RPO e RTO

Una configurazione HA mantiene un'elevata disponibilità dei dati come segue:

- L'obiettivo del punto di ripristino (RPO) è 0 secondi. I tuoi dati sono coerenti a livello transazionale e non subiscono perdite.
- L'obiettivo del tempo di recupero (RTO) è di 120 secondi. In caso di interruzione, i dati dovrebbero essere disponibili entro 120 secondi o meno.

Acquisizione e restituzione dello spazio di archiviazione

Analogamente a un cluster ONTAP fisico, lo storage in una coppia Azure HA è condiviso tra i nodi. Le connessioni allo storage del partner consentono a ciascun nodo di accedere allo storage dell'altro in caso di *acquisizione*. I meccanismi di failover del percorso di rete garantiscono che i client e gli host continuino a comunicare con il nodo superstite. Il partner *restituisce* spazio di archiviazione quando il nodo viene riportato online.

Per le configurazioni NAS, gli indirizzi IP dei dati migrano automaticamente tra i nodi HA in caso di guasti.

Per iSCSI, Cloud Volumes ONTAP utilizza Multipath I/O (MPIO) e Asymmetric Logical Unit Access (ALUA) per gestire il failover del percorso tra i percorsi ottimizzati attivi e quelli non ottimizzati.

> Per informazioni sulle configurazioni host specifiche che supportano ALUA, fare riferimento a "Strumento matrice di interoperabilità NetApp" e il "Guida agli host SAN e ai client cloud" per il sistema operativo host.

L'acquisizione, la risincronizzazione e la restituzione dello storage sono tutte operazioni automatiche per impostazione predefinita. Non è richiesta alcuna azione da parte dell'utente.

Configurazioni di archiviazione

È possibile utilizzare una coppia HA come configurazione attiva-attiva, in cui entrambi i nodi forniscono dati ai client, oppure come configurazione attiva-passiva, in cui il nodo passivo risponde alle richieste di dati solo se ha preso in carico lo storage per il nodo attivo.

Scopri di più sulle coppie Cloud Volumes ONTAP HA in Google Cloud

Una configurazione ad alta disponibilità (HA) Cloud Volumes ONTAP garantisce operazioni senza interruzioni e tolleranza agli errori. In Google Cloud, i dati vengono replicati in modo sincrono tra i due nodi.

Componenti HA

Le configurazioni Cloud Volumes ONTAP HA in Google Cloud includono i seguenti componenti:

- Due nodi Cloud Volumes ONTAP i cui dati vengono replicati in modo sincrono tra loro.
- Un'istanza di mediazione che fornisce un canale di comunicazione tra i nodi per agevolare i processi di acquisizione e restituzione dello storage.
- Una zona o tre zone (consigliato).

  Se si scelgono tre zone, i due nodi e il mediatore si trovano in zone Google Cloud separate.

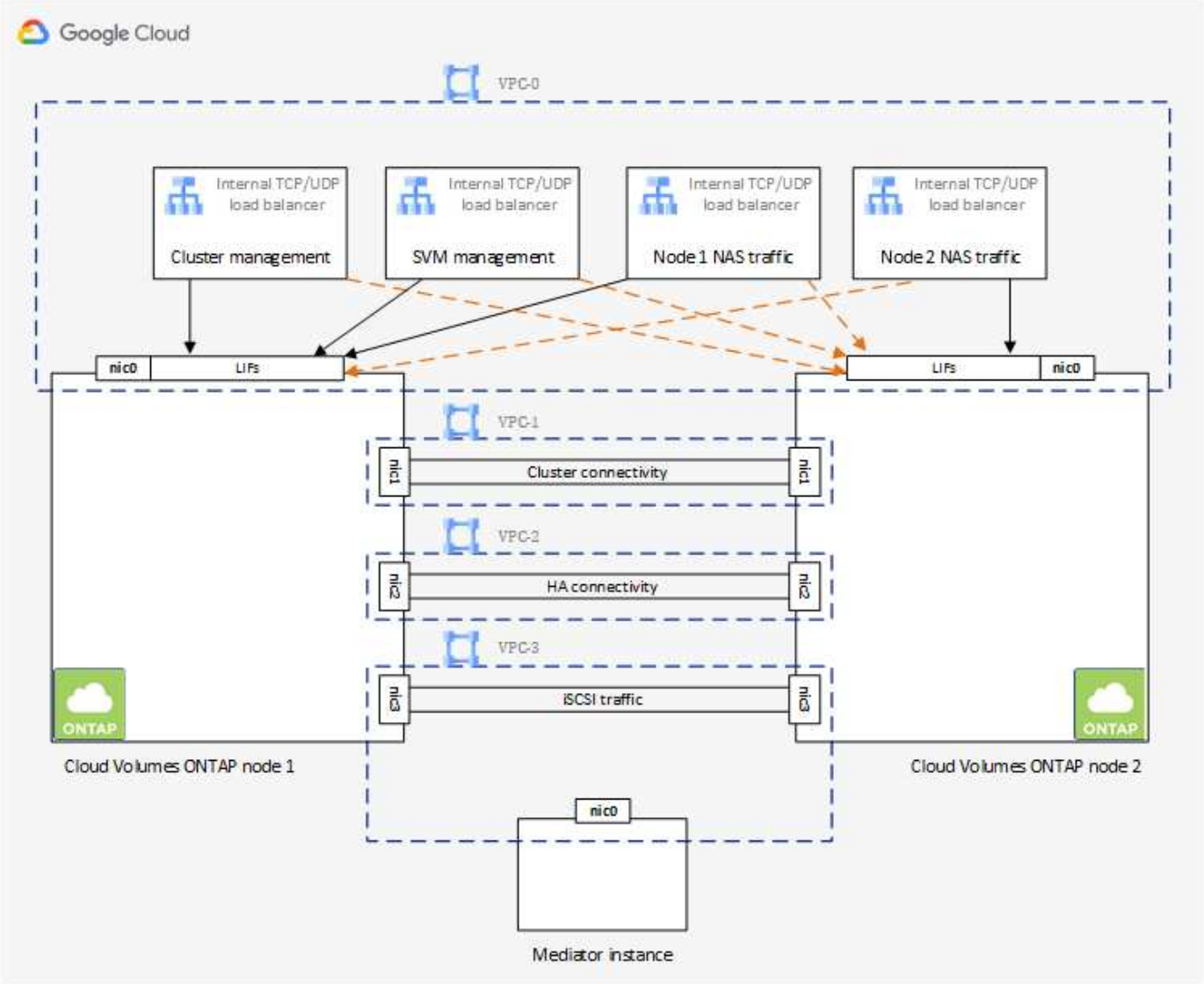
- Quattro Virtual Private Cloud (VPC).

  La configurazione utilizza quattro VPC perché GCP richiede che ogni interfaccia di rete risieda in una rete VPC separata.

- Quattro bilanciatori del carico interni di Google Cloud (TCP/UDP) che gestiscono il traffico in entrata verso la coppia Cloud Volumes ONTAP HA.

"Scopri i requisiti di rete", inclusi maggiori dettagli su bilanciatori di carico, VPC, indirizzi IP interni, subnet e altro ancora.

L'immagine concettuale seguente mostra una coppia Cloud Volumes ONTAP HA e i suoi componenti:



Mediatore

Ecco alcuni dettagli chiave sull'istanza del mediatore in Google Cloud:

Tipo di istanza

e2-micro (in precedenza era stata utilizzata un'istanza f1-micro)

Dischi

Due dischi persistenti standard da 10 GiB ciascuno

Sistema operativo

Debian 11

> Per Cloud Volumes ONTAP 9.10.0 e versioni precedenti, Debian 10 è stato installato sul mediatore.

Aggiornamenti

Quando si aggiorna Cloud Volumes ONTAP, la NetApp Console aggiorna anche l'istanza del mediatore in base alle necessità.

Accesso all'istanza

Per Debian, l'utente cloud predefinito è `admin`. Google Cloud crea e aggiunge un certificato per l'utente `admin` quando viene richiesto l'accesso SSH tramite Google Cloud Console o la riga di comando gcloud. Puoi specificare `sudo` per ottenere privilegi di root.

Agenti terzi

Gli agenti di terze parti o le estensioni VM non sono supportati sull'istanza del mediatore.

Acquisizione e restituzione dello spazio di archiviazione

Se un nodo si interrompe, l'altro nodo può fornire dati al suo partner per garantire la continuità del servizio dati. I client possono accedere agli stessi dati dal nodo partner perché i dati sono stati replicati in modo sincrono sul partner.

Dopo il riavvio del nodo, il partner deve risincronizzare i dati prima di poter restituire l'archiviazione. Il tempo necessario per risincronizzare i dati dipende dalla quantità di dati modificati mentre il nodo era inattivo.

L'acquisizione, la risincronizzazione e la restituzione dello storage sono tutte operazioni automatiche per impostazione predefinita. Non è richiesta alcuna azione da parte dell'utente.

RPO e RTO

Una configurazione HA mantiene un'elevata disponibilità dei dati come segue:

- L'obiettivo del punto di ripristino (RPO) è 0 secondi.

  I tuoi dati sono coerenti a livello transazionale e non subiscono perdite.

- L'obiettivo del tempo di recupero (RTO) è di 120 secondi.

  In caso di interruzione, i dati dovrebbero essere disponibili entro 120 secondi o meno.

Modelli di distribuzione HA

È possibile garantire l'elevata disponibilità dei dati distribuendo una configurazione HA in più zone o in una singola zona.

Zone multiple (consigliato)

L'implementazione di una configurazione HA su tre zone garantisce la disponibilità continua dei dati in caso di guasto in una zona. Si noti che le prestazioni di scrittura sono leggermente inferiori rispetto all'utilizzo di una singola zona, ma sono minime.

Zona singola

Quando distribuita in una singola zona, una configurazione Cloud Volumes ONTAP HA utilizza una politica di posizionamento distribuito. Questa politica garantisce che una configurazione HA sia protetta da un singolo punto di errore all'interno della zona, senza dover utilizzare zone separate per ottenere l'isolamento degli errori.

Questo modello di distribuzione riduce i costi perché non ci sono costi per l'uscita dei dati tra le zone.

Come funziona l'archiviazione in una coppia HA

A differenza di un cluster ONTAP , lo storage in una coppia Cloud Volumes ONTAP HA in GCP non è condiviso

tra i nodi. Al contrario, i dati vengono replicati in modo sincrono tra i nodi, in modo che siano disponibili anche in caso di guasto.

Assegnazione dello spazio di archiviazione

Quando si crea un nuovo volume e sono necessari dischi aggiuntivi, la Console alloca lo stesso numero di dischi a entrambi i nodi, crea un aggregato con mirroring e quindi crea il nuovo volume. Ad esempio, se per il volume sono necessari due dischi, la Console alloca due dischi per nodo, per un totale di quattro dischi.

Configurazioni di archiviazione

È possibile utilizzare una coppia HA come configurazione attiva-attiva, in cui entrambi i nodi forniscono dati ai client, oppure come configurazione attiva-passiva, in cui il nodo passivo risponde alle richieste di dati solo se ha preso in carico lo storage per il nodo attivo.

Aspettative di prestazioni per una configurazione HA

Una configurazione Cloud Volumes ONTAP HA replica in modo sincrono i dati tra i nodi, consumando larghezza di banda della rete. Di conseguenza, è possibile aspettarsi le seguenti prestazioni rispetto a una configurazione Cloud Volumes ONTAP a nodo singolo:

- Per le configurazioni HA che gestiscono dati da un solo nodo, le prestazioni di lettura sono paragonabili a quelle di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono inferiori.
- Per le configurazioni HA che gestiscono dati da entrambi i nodi, le prestazioni di lettura sono superiori rispetto a quelle di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono uguali o superiori.

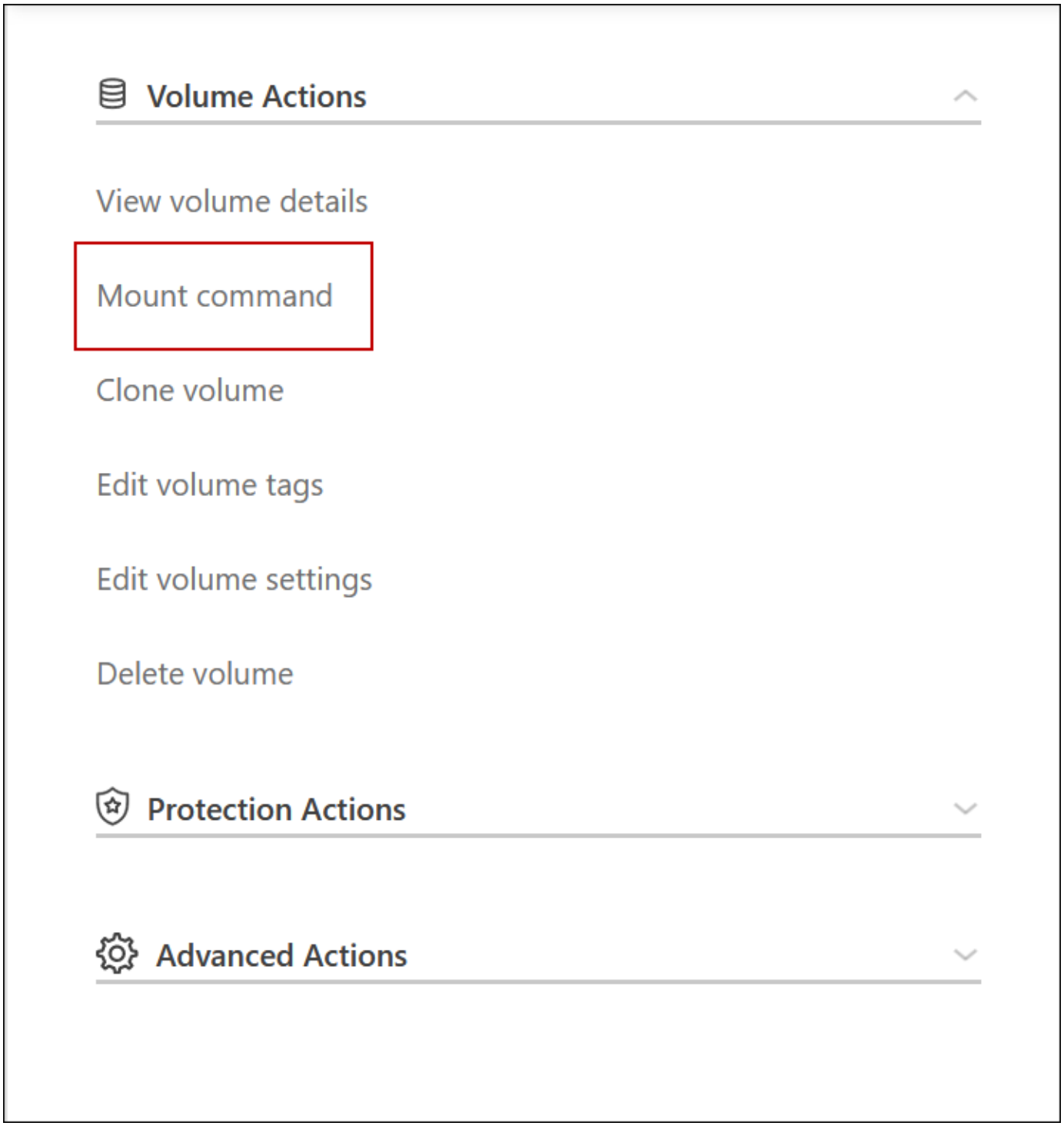
Per maggiori dettagli sulle prestazioni Cloud Volumes ONTAP , fare riferimento a"Prestazione" .

Accesso del cliente allo storage

I client devono accedere ai volumi NFS e CIFS utilizzando l'indirizzo IP dei dati del nodo su cui risiede il volume. Se i client NAS accedono a un volume utilizzando l'indirizzo IP del nodo partner, il traffico viene trasmesso tra entrambi i nodi, riducendo le prestazioni.

Se si sposta un volume tra nodi in una coppia HA, è necessario rimontare il volume utilizzando l'indirizzo IP dell'altro nodo. In caso contrario, le prestazioni potrebbero risultare ridotte. Se i client supportano i riferimenti NFSv4 o il reindirizzamento delle cartelle per CIFS, è possibile abilitare tali funzionalità sui sistemi Cloud Volumes ONTAP per evitare di dover rimontare il volume. Per maggiori dettagli, fare riferimento alla documentazione ONTAP .

È possibile individuare l'indirizzo IP corretto dalla Console selezionando il volume e facendo clic su **Comando di montaggio**.



Link correlati

- "Scopri i requisiti di rete"
- "Scopri come iniziare a usare GCP"

Operazioni non disponibili quando un nodo nella coppia Cloud Volumes ONTAP HA è offline

Quando un nodo in una coppia HA non è disponibile, l'altro nodo fornisce dati al partner per garantire un servizio dati continuo. Questo fenomeno è chiamato *acquisizione dello*

storage. Diverse azioni non saranno disponibili finché non sarà completata la restituzione in magazzino.

Quando un nodo in una coppia HA non è disponibile, lo stato del sistema nella NetApp Console è *Degradato*.

Le seguenti azioni non sono disponibili durante l'acquisizione dello storage:

- Registrazione del supporto
- Modifiche alla licenza
- Modifiche al tipo di istanza o VM
- Cambiamenti nella velocità di scrittura
- Configurazione CIFS
- Modifica della posizione dei backup di configurazione
- Impostazione della password del cluster
- Gestione di dischi e aggregati (allocazione avanzata)

Queste azioni saranno nuovamente disponibili una volta completata la restituzione dello spazio di archiviazione e quando lo stato del sistema tornerà alla normalità.

Scopri di più sulla crittografia dei dati e sulla protezione ransomware Cloud Volumes ONTAP

Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.

Crittografia dei dati a riposo

Cloud Volumes ONTAP supporta le seguenti tecnologie di crittografia:

- Soluzioni di crittografia NetApp (NVE e NAE)
- Servizio di gestione delle chiavi AWS
- Crittografia del servizio di archiviazione di Azure
- Crittografia predefinita di Google Cloud Platform

È possibile utilizzare le soluzioni di crittografia NetApp con la crittografia nativa del provider cloud, che crittografa i dati a livello di hypervisor. In questo modo si otterrebbe una doppia crittografia, che potrebbe essere utile per dati molto sensibili. Quando si accede ai dati crittografati, questi vengono decrittografati due volte: una volta a livello di hypervisor (utilizzando le chiavi del provider cloud) e un'altra volta utilizzando le soluzioni di crittografia NetApp (utilizzando le chiavi di un gestore di chiavi esterno).

Soluzioni di crittografia NetApp (NVE e NAE)

Cloud Volumes ONTAP supporta "Crittografia del volume NetApp (NVE) e crittografia aggregata NetApp (NAE)" . NVE e NAE sono soluzioni basate su software che consentono la crittografia dei dati a riposo dei volumi conforme allo standard (FIPS) 140-2. Sia NVE che NAE utilizzano la crittografia AES a 256 bit.

- NVE crittografa i dati inattivi un volume alla volta. Ogni volume di dati ha la sua chiave di crittografia univoca.
- NAE è un'estensione di NVE: crittografa i dati per ogni volume e i volumi condividono una chiave nell'aggregato. NAE consente inoltre di deduplicare i blocchi comuni in tutti i volumi dell'aggregato.

Cloud Volumes ONTAP supporta sia NVE che NAE con servizi di gestione delle chiavi esterne (EKM) forniti da AWS, Azure e Google Cloud, comprese soluzioni di terze parti come Fortanix. A differenza di ONTAP, per Cloud Volumes ONTAP le chiavi di crittografia vengono generate dal provider cloud, non in ONTAP. Cloud Volumes ONTAP non supporta "Responsabile delle chiavi di bordo".

Cloud Volumes ONTAP utilizza i servizi standard Key Management Interoperability Protocol (KMIP) utilizzati da ONTAP . Per maggiori informazioni sui servizi supportati, fare riferimento a "Strumento di matrice di interoperabilità" .

Se utilizzi NVE, hai la possibilità di utilizzare il key vault del tuo provider cloud per proteggere le chiavi di crittografia ONTAP :

- Servizio di gestione delle chiavi AWS (KMS)
- Azure Key Vault (AKV)
- Servizio di gestione delle chiavi di Google Cloud

Per impostazione predefinita, nei nuovi aggregati la crittografia NetApp Aggregate Encryption (NAE) è abilitata dopo aver configurato un gestore di chiavi esterno. Per impostazione predefinita, nei nuovi volumi che non fanno parte di un aggregato NAE, NVE è abilitato (ad esempio, se si dispone di aggregati esistenti creati prima di configurare un gestore di chiavi esterno).

L'unico passaggio obbligatorio è la configurazione di un gestore delle chiavi supportato. Per le istruzioni di configurazione, fare riferimento a"Crittografa i volumi con le soluzioni di crittografia NetApp" .

Servizio di gestione delle chiavi AWS

Quando si avvia un sistema Cloud Volumes ONTAP in AWS, è possibile abilitare la crittografia dei dati utilizzando "Servizio di gestione delle chiavi AWS (KMS)" . La NetApp Console richiede le chiavi dati utilizzando una chiave master del cliente (CMK).

Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP .

Se si desidera utilizzare questa opzione di crittografia, è necessario assicurarsi che AWS KMS sia configurato correttamente. Per informazioni, fare riferimento a"Configurazione di AWS KMS" .

Crittografia del servizio di archiviazione di Azure

I dati vengono crittografati automaticamente su Cloud Volumes ONTAP in Azure utilizzando "Crittografia del servizio di archiviazione di Azure" con una chiave gestita da Microsoft.

Se preferisci, puoi utilizzare le tue chiavi di crittografia. "Scopri come configurare Cloud Volumes ONTAP per utilizzare una chiave gestita dal cliente in Azure" .

Crittografia predefinita di Google Cloud Platform

"Crittografia dei dati inattivi di Google Cloud Platform"è abilitato per impostazione predefinita per Cloud Volumes ONTAP. Non è richiesta alcuna configurazione.

Sebbene Google Cloud Storage crittografi sempre i dati prima che vengano scritti sul disco, è possibile utilizzare le API della console per creare un sistema Cloud Volumes ONTAP che utilizzi *chiavi di crittografia gestite dal cliente*. Si tratta di chiavi che puoi generare e gestire in GCP utilizzando Cloud Key Management Service. "Saperne di più" .

Scansione antivirus ONTAP

È possibile utilizzare la funzionalità antivirus integrata nei sistemi ONTAP per proteggere i dati dalla compromissione da parte di virus o altri codici dannosi.

La scansione antivirus ONTAP , denominata *Vscan*, combina il miglior software antivirus di terze parti con le funzionalità ONTAP che ti offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

Per informazioni sui fornitori, sul software e sulle versioni supportate da Vscan, fare riferimento a "Matrice di interoperabilità NetApp" .

Per informazioni su come configurare e gestire la funzionalità antivirus sui sistemi ONTAP , fare riferimento a "Guida alla configurazione dell'antivirus ONTAP 9" .

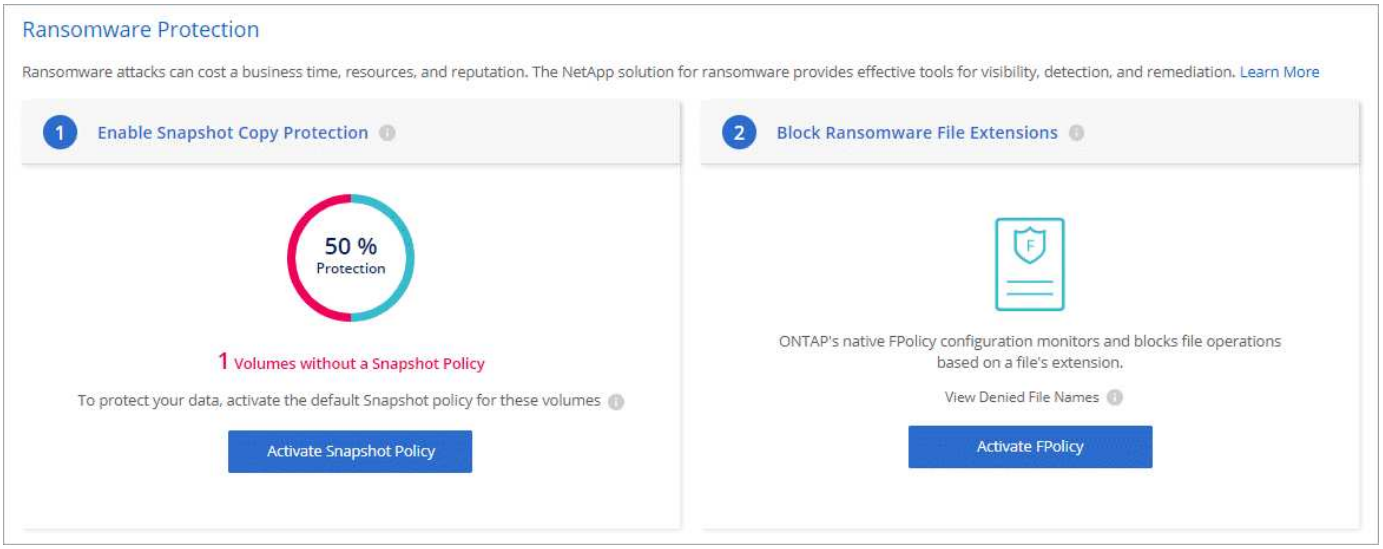
Protezione dal ransomware

Gli attacchi ransomware possono costare alle aziende tempo, risorse e reputazione. La Console consente di implementare la soluzione NetApp per il ransomware, che fornisce strumenti efficaci per la visibilità, il rilevamento e la correzione.

- La Console identifica i volumi che non sono protetti da un criterio Snapshot e consente di attivare il criterio Snapshot predefinito su tali volumi.

  Le copie snapshot sono di sola lettura, il che impedisce la corruzione da parte del ransomware. Possono anche fornire la granularità necessaria per creare immagini di una singola copia di file o una soluzione completa di disaster recovery.

- La Console consente inoltre di bloccare le estensioni di file ransomware più comuni abilitando la soluzione FPolicy di ONTAP.



"Scopri come implementare la soluzione NetApp contro il ransomware" .

Scopri di più sul monitoraggio delle prestazioni per i carichi di lavoro Cloud Volumes ONTAP

È possibile esaminare i risultati delle prestazioni per decidere quali carichi di lavoro sono appropriati per Cloud Volumes ONTAP.

Rapporti tecnici sulle prestazioni

- Cloud Volumes ONTAP per AWS

  "Rapporto tecnico NetApp 4383: Caratterizzazione delle prestazioni di Cloud Volumes ONTAP in Amazon Web Services con carichi di lavoro applicativi"

- Cloud Volumes ONTAP per Microsoft Azure

  "Report tecnico NetApp 4671: caratterizzazione delle prestazioni di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi"

- Cloud Volumes ONTAP per Google Cloud

  "Rapporto tecnico NetApp 4816: Caratterizzazione delle prestazioni di Cloud Volumes ONTAP per Google Cloud"

Prestazioni della CPU

I nodi Cloud Volumes ONTAP risultano altamente utilizzati (oltre il 90%) dagli strumenti di monitoraggio del tuo provider cloud. Ciò avviene perché ONTAP riserva tutte le vCPU presentate alla macchina virtuale, in modo che siano disponibili quando necessario.

Per informazioni fare riferimento al "Articolo della knowledge base NetApp su come monitorare l'utilizzo della CPU ONTAP tramite la CLI"

Gestione delle licenze per BYOL basato su nodi

Ogni sistema Cloud Volumes ONTAP dotato di licenza BYOL (Bring Your Own License) basata su nodi deve disporre di una licenza di sistema installata con un abbonamento attivo. NetApp Console semplifica il processo gestendo le licenze per te e visualizzando un avviso prima della loro scadenza.

> Una licenza basata su nodi è la licenza di precedente generazione per Cloud Volumes ONTAP. Una licenza basata su nodi può essere acquistata da NetApp (BYOL) ed è disponibile per i rinnovi di licenza solo in casi specifici.

"Scopri di più sulle opzioni di licenza Cloud Volumes ONTAP" .

"Scopri di più su come gestire le licenze basate sui nodi" .

Licenze del sistema BYOL

Le licenze basate su nodi possono essere acquistate da NetApp. Il numero di licenze che puoi acquistare per

un sistema a nodo singolo o una coppia HA è illimitato.

NetApp ha limitato l'acquisto, l'estensione e il rinnovo delle licenze BYOL. Per ulteriori informazioni, consulta "Disponibilità limitata delle licenze BYOL per Cloud Volumes ONTAPP" .

Una licenza basata su nodi fornisce fino a 368 TiB di capacità per un singolo nodo o una coppia HA. Potresti aver acquistato più licenze per un sistema BYOL Cloud Volumes ONTAP per allocare più di 368 TiB di capacità. Ad esempio, potresti avere due licenze per allocare fino a 736 TiB di capacità a Cloud Volumes ONTAP. Oppure potresti avere quattro licenze per ottenere fino a 1,4 PiB.

Tieni presente che i limiti del disco possono impedirti di raggiungere il limite di capacità utilizzando solo i dischi. Puoi superare il limite del disco"suddivisione in livelli dei dati inattivi nell'archiviazione degli oggetti" . Per informazioni sui limiti del disco, fare riferimento a "limiti di archiviazione nelle note di rilascio di Cloud Volumes ONTAP" .

Gestione delle licenze per un nuovo sistema

Quando si crea un sistema BYOL basato su nodi, la Console richiede il numero di serie della licenza e l'account del sito di supporto NetApp . La console utilizza l'account per scaricare il file di licenza da NetApp e installarlo sul sistema Cloud Volumes ONTAP .

"Scopri come aggiungere account del sito di supporto NetApp alla console" .

Se la console non riesce ad accedere al file di licenza tramite la connessione Internet protetta, è possibile"ottenere il file da soli e poi caricarlo manualmente sulla Console" .

Scadenza della licenza

La Console visualizza un avviso 30 giorni prima della scadenza di una licenza basata su nodo e nuovamente alla scadenza della licenza. L'immagine seguente mostra un avviso di scadenza di 30 giorni che appare nell'interfaccia utente:

È possibile selezionare il sistema per rivedere il messaggio.

La Console include un avviso di scadenza della licenza nel report Cloud Volumes ONTAP che ti viene inviato tramite e-mail, se sei un amministratore dell'organizzazione o dell'account e hai abilitato l'opzione. Il report inviato via e-mail include l'avviso di scadenza della licenza ogni 2 settimane.

Se non si rinnova la licenza in tempo, il sistema Cloud Volumes ONTAP si arresta automaticamente. Se lo riavvii, si spegne di nuovo.

Rinnovo della licenza

Se si rinnova un abbonamento BYOL basato su nodi contattando un rappresentante NetApp , la Console ottiene automaticamente la nuova licenza da NetApp e la installa sul sistema Cloud Volumes ONTAP .

Se la console non riesce ad accedere al file di licenza tramite la connessione Internet protetta, è possibile"ottenere il file da soli e poi caricarlo manualmente sulla Console" .

Trasferimento della licenza a un nuovo sistema

Una licenza BYOL basata su nodi è trasferibile tra sistemi Cloud Volumes ONTAP quando si elimina un sistema esistente e poi ne si crea uno nuovo utilizzando la stessa licenza.

Ad esempio, potresti voler eliminare un sistema con licenza esistente e quindi utilizzare la licenza con un nuovo sistema BYOL in un diverso provider VPC/VNet o cloud. Tieni presente che solo i numeri di serie *cloud-agnostic* funzionano con qualsiasi provider cloud. I numeri di serie indipendenti dal cloud iniziano con il prefisso *908xxxx*.

È importante notare che la licenza BYOL è legata alla tua azienda e a un set specifico di credenziali del sito di supporto NetApp .

Scopri come AutoSupport e Digital Advisor vengono utilizzati per Cloud Volumes ONTAP

Il componente AutoSupport di ONTAP raccoglie i dati di telemetria e li invia per l'analisi. Active IQ Digital Advisor (noto anche come Digital Advisor) analizza i dati di AutoSupport e fornisce assistenza e ottimizzazione proattive. Utilizzando l'intelligenza artificiale, Digital Advisor può identificare potenziali problemi e aiutarti a risolverli prima che abbiano ripercussioni sulla tua attività.

Digital Advisor ti consente di ottimizzare la tua infrastruttura dati nel tuo cloud ibrido globale offrendo analisi predittive fruibili e supporto proattivo tramite un portale basato su cloud e un'app mobile. Le informazioni e le raccomandazioni basate sui dati di Digital Advisor sono disponibili per tutti i clienti NetApp con un contratto SupportEdge attivo (le funzionalità variano in base al prodotto e al livello di supporto).

Ecco alcune cose che puoi fare con Digital Advisor:

- Pianificare gli aggiornamenti.

  Digital Advisor individua i problemi nel tuo ambiente che possono essere risolti aggiornando a una versione più recente di ONTAP e il componente Upgrade Advisor ti aiuta a pianificare un aggiornamento riuscito.

- Visualizza il benessere del sistema.

  La dashboard del tuo Digital Advisor segnala eventuali problemi relativi al benessere e ti aiuta a risolverli. Monitora la capacità del sistema per assicurarti di non rimanere mai senza spazio di archiviazione. Visualizza i casi di supporto per il tuo sistema.

- Gestire le prestazioni.

  Digital Advisor mostra le prestazioni del sistema per un periodo di tempo più lungo di quello visualizzabile in ONTAP System Manager. Identifica i problemi di configurazione e di sistema che incidono sulle tue prestazioni. Massimizzare l'efficienza. Visualizza le metriche di efficienza dell'archiviazione e identifica i modi per archiviare più dati in meno spazio.

- Visualizza inventario e configurazione.

Digital Advisor visualizza informazioni complete sull'inventario e sulla configurazione software e hardware. Controlla quando scadono i contratti di servizio e rinnovali per assicurarti di continuare a ricevere supporto.

Link correlati

- "Documentazione NetApp : Digital Advisor"
- "Avvia il Digital Advisor"
- "Servizi SupportEdge"

Configurazioni predefinite supportate per Cloud Volumes ONTAP

Comprendere come Cloud Volumes ONTAP è configurato per impostazione predefinita può aiutarti a configurare e amministrare i tuoi sistemi, soprattutto se hai familiarità con ONTAP , perché la configurazione predefinita per Cloud Volumes ONTAP è diversa da quella di ONTAP.

Configurazione predefinita

- La NetApp Console crea una VM di storage per la gestione dei dati quando distribuisce Cloud Volumes ONTAP. Alcune configurazioni supportano VM di archiviazione aggiuntive. "Scopri di più sulla gestione delle VM di archiviazione" .

  A partire dalla versione 3.9.5, la segnalazione dello spazio logico è abilitata sulla VM di archiviazione iniziale. Quando lo spazio viene segnalato in modo logico, ONTAP segnala lo spazio del volume in modo tale che tutto lo spazio fisico risparmiato dalle funzionalità di efficienza di archiviazione venga segnalato come utilizzato. Per informazioni sulle funzionalità di efficienza dell'archiviazione in linea, fare riferimento all'articolo della knowledge base "KB: Quali funzionalità di Inline Storage Efficiency sono supportate da CVO?"

- La Console installa automaticamente le seguenti licenze delle funzionalità ONTAP su Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - Gestione delle chiavi di crittografia multi-tenant (MTEKM), a partire da Cloud Volumes ONTAP 9.12.1 GA
  - NetApp Volume Encryption (solo per sistemi BYOL (Bring Your Own License) o PAYGO (Registered Pay-as-You-Go))
  - NFS ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]
  - SnapMirror
  - SnapRestore
  - SnapVault
- Per impostazione predefinita vengono create diverse interfacce di rete:
  - Un LIF di gestione dei cluster

    - Un LIF intercluster
- Un LIF di gestione SVM su sistemi HA in Azure
- Un LIF di gestione SVM su sistemi HA in Google Cloud
- Un LIF di gestione SVM su sistemi a nodo singolo in AWS
- Un LIF di gestione dei nodi

+ In Google Cloud, questo LIF è combinato con il LIF intercluster.

- Un LIF di dati iSCSI
- Un LIF di dati CIFS e NFS

> Per impostazione predefinita, il failover LIF è disabilitato per Cloud Volumes ONTAP a causa dei requisiti del provider cloud. La migrazione di un LIF su una porta diversa interrompe la mappatura esterna tra indirizzi IP e interfacce di rete sull'istanza, rendendo il LIF inaccessibile.

    - Cloud Volumes ONTAP invia i backup della configurazione all'agente della console tramite HTTP.

      I backup sono accessibili da http://ipaddress/occm/offboxconfig/ dove *ipaddress* è l'indirizzo IP dell'host dell'agente Console.

      È possibile utilizzare i backup per riconfigurare il sistema Cloud Volumes ONTAP . Per ulteriori informazioni sui backup di configurazione, fare riferimento a "Documentazione ONTAP" .

    - La Console imposta alcuni attributi del volume in modo diverso rispetto ad altri strumenti di gestione (ad esempio ONTAP System Manager o ONTAP CLI).

      Nella tabella seguente sono elencati gli attributi del volume impostati in modo diverso dai valori predefiniti:

Attributo	Valore che la Console configura
Modalità di ridimensionamento automatico	crescere
Dimensione automatica massima	1.000 percento L'amministratore dell'organizzazione o dell'account può modificare questo valore dalla pagina Impostazioni.
Stile di sicurezza	NTFS per volumi CIFS UNIX per volumi NFS
Stile di garanzia dello spazio	nessuno
Permessi UNIX (solo NFS)	777

+
Per informazioni su questi attributi, fare riferimento a"Pagina man ONTAP *volume create*" .

Dischi interni per i dati di sistema

Oltre allo spazio di archiviazione per i dati utente, la Console acquista anche spazio di archiviazione cloud per i dati di sistema.

AWS

- Tre dischi per nodo per dati di avvio, root e core:
  - Disco io1 da 47 GiB per i dati di avvio
  - Disco gp3 da 140 GiB per i dati di root
  - Disco gp2 da 540 GiB per i dati principali
- Per coppie HA:
  - Due volumi EBS st1 per l'istanza del mediatore, uno di circa 8 GiB come disco radice e uno di 4 GiB come disco dati
  - Un disco gp3 da 140 GiB in ogni nodo per contenere una copia dei dati radice dell'altro nodo

    In alcune zone, il tipo di disco EBS disponibile può essere solo gp2.
- Uno snapshot EBS per ogni disco di avvio e disco di root

  Gli snapshot vengono creati automaticamente al riavvio.
- Quando si abilita la crittografia dei dati in AWS tramite Key Management Service (KMS), vengono crittografati anche i dischi di avvio e root per Cloud Volumes ONTAP . Ciò include il disco di avvio per l'istanza del mediatore in una coppia HA. I dischi vengono crittografati utilizzando la CMK selezionata quando si aggiunge un sistema Cloud Volumes ONTAP .

In AWS, la NVRAM si trova sul disco di avvio.

Azure (nodo singolo)

- Tre dischi SSD Premium:
  - Un disco da 10 GiB per i dati di avvio
  - Un disco da 140 GiB per i dati di root
  - Un disco da 512 GiB per NVRAM

    Se la macchina virtuale scelta per Cloud Volumes ONTAP supporta Ultra SSD, il sistema utilizza un Ultra SSD da 32 GiB per NVRAM anziché un Premium SSD.
- Un disco HDD standard da 1024 GiB per il salvataggio dei core
- Uno snapshot di Azure per ogni disco di avvio e disco radice
- Per impostazione predefinita, in Azure ogni disco è crittografato quando è inattivo.

  Se la macchina virtuale scelta per Cloud Volumes ONTAP supporta Premium SSD v2 Managed Disk come

disco dati, il sistema utilizza un Premium SSD v2 Managed Disk da 32 GiB per la NVRAM e un altro come disco radice.

Azzurro (coppia HA)

HA si abbina al blob di pagina

- Due dischi SSD Premium da 10 GiB per il volume di avvio (uno per nodo)
- Due blob di pagina Premium Storage da 140 GiB per il volume radice (uno per nodo)
- Due dischi HDD standard da 1024 GiB per il salvataggio dei core (uno per nodo)
- Due dischi SSD Premium da 512 GiB per NVRAM (uno per nodo)
- Uno snapshot di Azure per ogni disco di avvio e disco radice

  Gli snapshot vengono creati automaticamente al riavvio.

- Per impostazione predefinita, in Azure ogni disco è crittografato quando è inattivo.

Coppie HA con dischi gestiti condivisi in più zone di disponibilità

- Due dischi SSD Premium da 10 GiB per il volume di avvio (uno per nodo)
- Due dischi SSD Premium da 512 GiB per il volume root (uno per nodo)
- Due dischi HDD standard da 1024 GiB per il salvataggio dei core (uno per nodo)
- Due dischi SSD Premium da 512 GiB per NVRAM (uno per nodo)
- Uno snapshot di Azure per ogni disco di avvio e disco radice

  Gli snapshot vengono creati automaticamente al riavvio.

- Per impostazione predefinita, in Azure ogni disco è crittografato quando è inattivo.

Coppie HA con dischi gestiti condivisi in singole zone di disponibilità

- Due dischi SSD Premium da 10 GiB per il volume di avvio (uno per nodo)
- Due dischi condivisi gestiti SSD Premium da 512 GiB per il volume root (uno per nodo)
- Due dischi HDD standard da 1024 GiB per il salvataggio dei core (uno per nodo)
- Due dischi gestiti SSD Premium da 512 GiB per NVRAM (uno per nodo)

Se la macchina virtuale supporta i dischi gestiti Premium SSD v2 come dischi dati, utilizza dischi gestiti Premium SSD v2 da 32 GiB per NVRAM e dischi gestiti condivisi Premium SSD v2 da 512 GiB per il volume root.

È possibile distribuire coppie HA in un'unica zona di disponibilità e utilizzare Premium SSD v2 Managed Disks quando sono soddisfatte le seguenti condizioni:

- La versione di Cloud Volumes ONTAP è 9.15.1 o successiva.
- La regione e la zona selezionate supportano i dischi gestiti Premium SSD v2. Per informazioni sulle regioni supportate, fare riferimento a "Sito Web di Microsoft Azure: prodotti disponibili per regione" .
- L'abbonamento è registrato per Microsoft"Funzionalità Microsoft.Compute/VMOrchestratorZonalMultiFD" .

Google Cloud (nodo singolo)

- Un disco persistente SSD da 10 GiB per i dati di avvio
- Un disco persistente SSD da 64 GiB per i dati di root
- Un disco persistente SSD da 500 GiB per NVRAM
- Un disco persistente standard da 315 GiB per il salvataggio dei core
- Snapshot per i dati di avvio e root

  Gli snapshot vengono creati automaticamente al riavvio.

- Per impostazione predefinita, i dischi di avvio e di root sono crittografati.

Google Cloud (coppia HA)

- Due dischi persistenti SSD da 10 GiB per i dati di avvio
- Quattro dischi SSD persistenti da 64 GiB per i dati di root
- Due dischi persistenti SSD da 500 GiB per NVRAM
- Due dischi persistenti standard da 315 GiB per il salvataggio dei core
- Un disco persistente standard da 10 GiB per i dati del mediatore
- Un disco persistente standard da 10 GiB per i dati di avvio del mediatore
- Snapshot per i dati di avvio e root

  Gli snapshot vengono creati automaticamente al riavvio.

- Per impostazione predefinita, i dischi di avvio e di root sono crittografati.

Dove risiedono i dischi

Disposizione dello spazio di archiviazione:

- I dati di avvio risiedono su un disco collegato all'istanza o alla macchina virtuale.

  Questo disco, che contiene l'immagine di avvio, non è disponibile per Cloud Volumes ONTAP.

- I dati radice, che contengono la configurazione e i registri del sistema, risiedono in aggr0.
- Il volume radice della macchina virtuale di archiviazione (SVM) risiede in aggr1.
- I volumi di dati risiedono anche in aggr1.

Conoscenza e supporto

Registrati per ricevere supporto

Per ricevere supporto tecnico specifico per NetApp Console e le sue soluzioni di storage e servizi dati è necessaria la registrazione al supporto. La registrazione del supporto è inoltre richiesta per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP .

La registrazione per il supporto non abilita il supporto NetApp per un servizio file del provider cloud. Per assistenza tecnica relativa a un servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla sezione "Ottenere assistenza" nella documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Panoramica della registrazione del supporto

Per attivare il diritto al sostegno sono previste due modalità di registrazione:

- Registrando il numero di serie del tuo account NetApp Console (il numero di serie di 20 cifre 960xxxxxxxx che si trova nella pagina Risorse di supporto nella Console).

  Questo funge da ID di abbonamento unico per qualsiasi servizio all'interno della Console. Ogni account Console deve essere registrato.

- Registrazione dei numeri di serie di Cloud Volumes ONTAP associati a un abbonamento nel marketplace del tuo provider cloud (si tratta di numeri di serie a 20 cifre 909201xxxxxxxx).

  Questi numeri di serie sono comunemente denominati *numeri di serie PAYGO* e vengono generati dalla NetApp Console al momento della distribuzione Cloud Volumes ONTAP .

La registrazione di entrambi i tipi di numeri di serie consente funzionalità quali l'apertura di ticket di supporto e la generazione automatica di casi. La registrazione viene completata aggiungendo gli account NetApp Support Site (NSS) alla Console come descritto di seguito.

Registra NetApp Console per il supporto NetApp

Per registrarsi per ricevere supporto e attivare il diritto al supporto, un utente del tuo account NetApp Console deve associare un account NetApp Support Site al proprio accesso alla Console. La modalità di registrazione per l'assistenza NetApp varia a seconda che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite la Console.

Passi

1. Selezionare **Amministrazione** > **Credenziali**.

2. Selezionare **Credenziali utente**.
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp (NSS).
4. Per confermare che il processo di registrazione è andato a buon fine, seleziona l'icona Aiuto e poi **Supporto**.

   La pagina **Risorse** dovrebbe mostrare che il tuo account Console è registrato per il supporto.

   Tieni presente che gli altri utenti della Console non vedranno lo stesso stato di registrazione del supporto se non hanno associato un account NetApp Support Site al loro login. Tuttavia, ciò non significa che il tuo account non sia registrato per l'assistenza. Se un utente dell'organizzazione ha seguito questi passaggi, il tuo account è stato registrato.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp esistente con licenze e numeri di serie esistenti ma *nessun* account NSS, devi creare un account NSS e associarlo al tuo accesso alla Console.

Passi

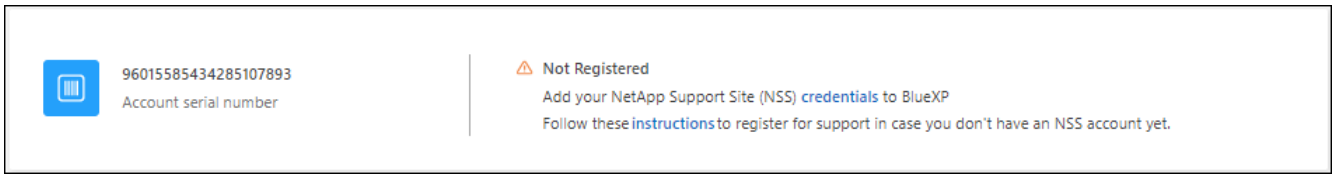
1. Crea un account del sito di supporto NetApp completando il "Modulo di registrazione utente del sito di supporto NetApp"
   a. Assicurati di selezionare il livello utente appropriato, che in genere è **Cliente NetApp /Utente finale**.
   b. Assicurati di copiare il numero di serie dell'account della console (960xxxx) utilizzato sopra per il campo del numero di serie. Ciò velocizzerà l'elaborazione dell'account.
2. Associa il tuo nuovo account NSS al tuo accesso alla Console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Novità assoluta per NetApp

Se sei un nuovo utente NetApp e non hai un account NSS, segui i passaggi indicati di seguito.

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.
2. Individua il numero di serie del tuo ID account nella pagina di registrazione del supporto.



3. Vai a "Sito di registrazione del supporto NetApp" e seleziona **Non sono un cliente NetApp registrato**.
4. Compila i campi obbligatori (quelli contrassegnati da asterischi rossi).
5. Nel campo **Linea di prodotti**, seleziona **Cloud Manager** e poi seleziona il tuo fornitore di fatturazione applicabile.
6. Copia il numero di serie del tuo account dal passaggio 2 sopra, completa il controllo di sicurezza e conferma di aver letto l'Informativa globale sulla privacy dei dati di NetApp.

   Per finalizzare questa transazione sicura, verrà inviata immediatamente un'e-mail alla casella di posta indicata. Se l'e-mail di convalida non arriva entro pochi minuti, assicurati di controllare la cartella spam.

7. Conferma l'azione dall'interno dell'e-mail.

   La conferma invia la richiesta a NetApp e ti consiglia di creare un account sul sito di supporto NetApp .

8. Crea un account del sito di supporto NetApp completando il "Modulo di registrazione utente del sito di supporto NetApp"
   a. Assicurati di selezionare il livello utente appropriato, che in genere è **Cliente NetApp /Utente finale**.
   b. Assicurati di copiare il numero di serie dell'account (960xxxx) utilizzato sopra per il campo del numero di serie. Ciò velocizzerà l'elaborazione.

Dopo aver finito

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di onboarding una tantum per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp , associalo al tuo accesso alla console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

L'associazione delle credenziali del sito di supporto NetApp al tuo account della console è necessaria per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- Registrazione dei sistemi Cloud Volumes ONTAP a consumo per il supporto

  Per attivare il supporto per il tuo sistema e accedere alle risorse di supporto tecnico NetApp è necessario fornire il tuo account NSS.

- Distribuzione di Cloud Volumes ONTAP quando si utilizza la propria licenza (BYOL)

  È necessario fornire il proprio account NSS affinché la Console possa caricare la chiave di licenza e abilitare l'abbonamento per il periodo acquistato. Ciò include aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP all'ultima versione

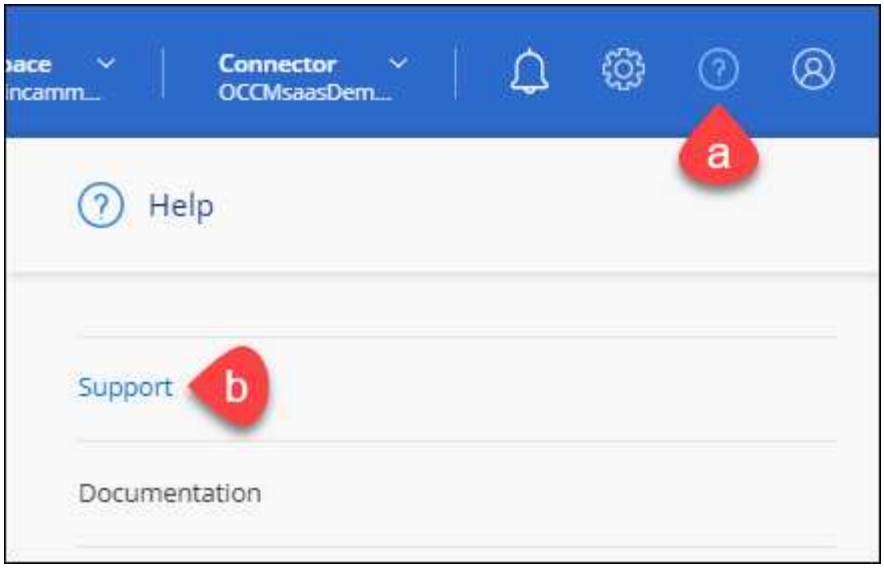
L'associazione delle credenziali NSS al tuo account NetApp Console è diversa dall'associazione dell'account NSS all'accesso utente della Console.

Queste credenziali NSS sono associate al tuo ID account Console specifico. Gli utenti che appartengono all'organizzazione Console possono accedere a queste credenziali da **Supporto > Gestione NSS**.

- Se disponi di un account a livello cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o rivenditore, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, seleziona **Continua** per essere reindirizzato alla pagina di accesso di Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e le licenze.

4. Nella pagina di accesso, inserisci l'indirizzo email e la password registrati sul sito di supporto NetApp per eseguire il processo di autenticazione.

   Queste azioni consentono alla Console di utilizzare il tuo account NSS per attività quali download di licenze, verifica di aggiornamenti software e future registrazioni di supporto.

   Notare quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account ospite o temporaneo). È possibile avere più account NSS a livello di cliente.
   - Può esserci un solo account NSS se tale account è un account a livello di partner. Se provi ad aggiungere account NSS a livello di cliente ed esiste già un account a livello di partner, riceverai il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account poiché sono già presenti utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS preesistenti a livello di cliente e si tenta di aggiungere un account a livello di partner.

   - Dopo aver effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che corrisponde al tuo indirizzo email. Nella pagina **Gestione NSS**, puoi visualizzare la tua email da ••• menu.

   - Se hai bisogno di aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Aggiorna credenziali** in ••• menu.

     Utilizzando questa opzione ti verrà richiesto di effettuare nuovamente l'accesso. Si noti che il token per questi account scade dopo 90 giorni. Verrà pubblicata una notifica per avvisarti di ciò.

Ottieni aiuto

NetApp fornisce supporto per NetApp Console e i suoi servizi cloud in vari modi. Sono disponibili ampie opzioni di auto-supporto gratuite 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include supporto tecnico remoto tramite ticket web.

Ottieni supporto per un servizio file di un provider cloud

Per il supporto tecnico relativo al servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Per ricevere supporto tecnico specifico per NetApp e le sue soluzioni di storage e servizi dati, utilizzare le opzioni di supporto descritte di seguito.

Utilizzare opzioni di auto-supporto

Queste opzioni sono disponibili gratuitamente, 24 ore al giorno, 7 giorni alla settimana:

- Documentazione

  La documentazione NetApp Console che stai visualizzando.

- "Base di conoscenza"

  Cerca nella knowledge base NetApp per trovare articoli utili per la risoluzione dei problemi.

- "Comunità"

  Unisciti alla community NetApp Console per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo aver attivato il supporto.

Prima di iniziare

- Per utilizzare la funzionalità **Crea un caso**, devi prima associare le credenziali del sito di supporto NetApp all'accesso alla console. "Scopri come gestire le credenziali associate al tuo accesso alla Console" .
- Se stai aprendo un caso per un sistema ONTAP che ha un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Nella pagina **Risorse**, seleziona una delle opzioni disponibili in Supporto tecnico:

a. Seleziona **Chiamaci** se desideri parlare con qualcuno al telefono. Verrai indirizzato a una pagina su netapp.com in cui sono elencati i numeri di telefono che puoi chiamare.

b. Seleziona **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp :

   - **Servizio**: seleziona il servizio a cui è associato il problema. Ad esempio, * NetApp Console* quando si tratta di un problema specifico di supporto tecnico con flussi di lavoro o funzionalità all'interno della Console.
   - **Sistema**: se applicabile all'archiviazione, selezionare * Cloud Volumes ONTAP* o **On-Prem** e quindi l'ambiente di lavoro associato.

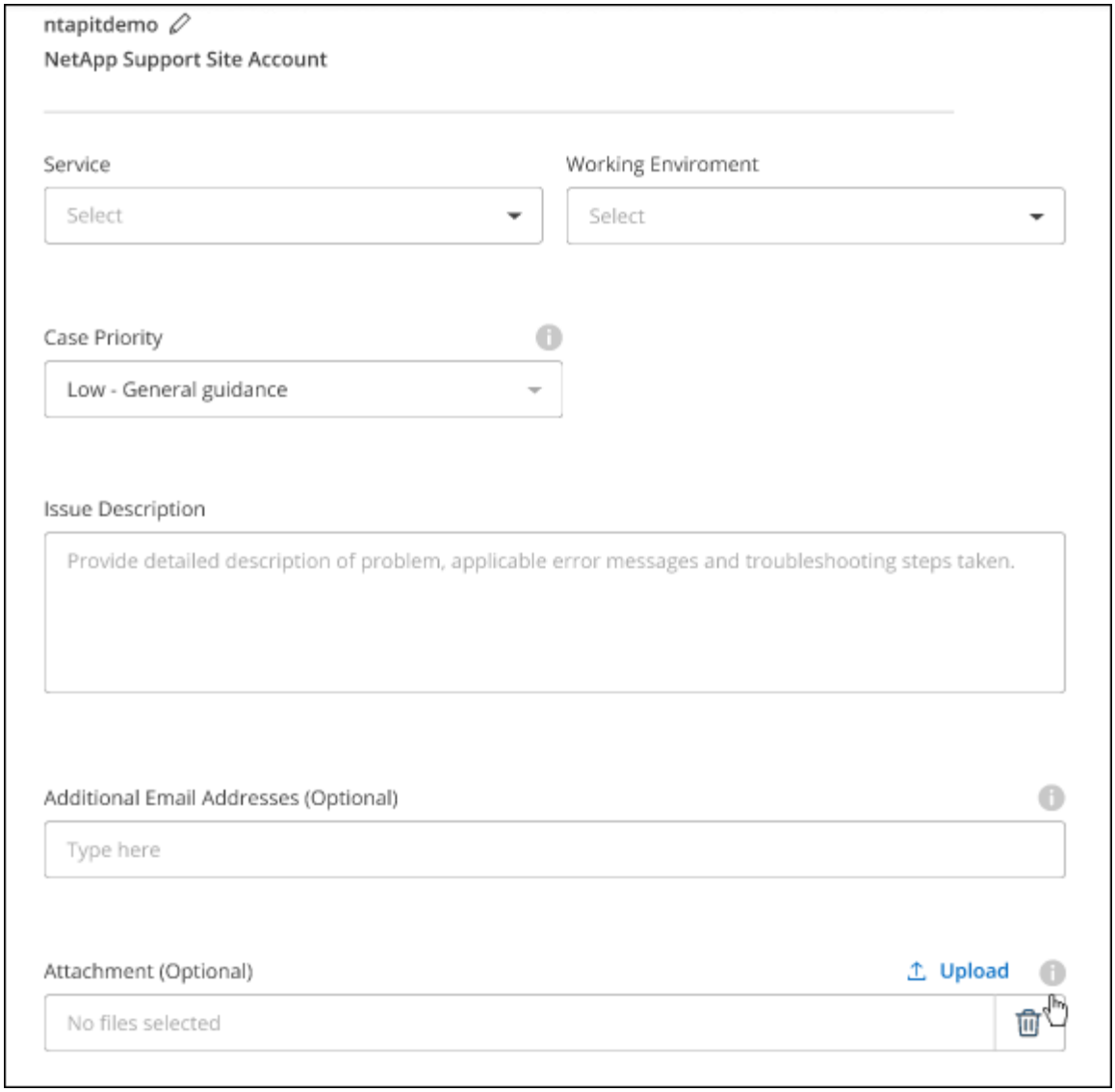
     L'elenco dei sistemi rientra nell'ambito dell'organizzazione della Console e dell'agente della Console selezionato nel banner in alto.

   - **Priorità del caso**: scegli la priorità del caso, che può essere Bassa, Media, Alta o Critica.

     Per saperne di più su queste priorità, passa il mouse sull'icona informativa accanto al nome del campo.

   - **Descrizione del problema**: fornisci una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o passaggi per la risoluzione dei problemi eseguiti.
   - **Indirizzi email aggiuntivi**: inserisci altri indirizzi email se desideri informare qualcun altro di questo problema.
   - **Allegato (facoltativo)**: carica fino a cinque allegati, uno alla volta.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Dopo aver finito

Apparirà una finestra pop-up con il numero del tuo caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei tuoi casi di supporto, puoi selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzarne i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso contro il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società registrata a cui è associato non corrispondono alla stessa società registrata per il numero di serie dell'account NetApp Console (ad esempio 960xxxx) o il numero di serie dell'ambiente di lavoro. Puoi richiedere assistenza utilizzando una delle seguenti opzioni:

- Invia un caso non tecnico a https://mysupport.netapp.com/site/help

Gestisci i tuoi casi di supporto

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente dalla Console. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

Notare quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base al tuo account NSS utente.

  I risultati nella tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come Priorità e Stato. Altre colonne forniscono solo funzionalità di ordinamento.

  Per maggiori dettagli, vedere i passaggi riportati di seguito.
- A livello di singolo caso, offriamo la possibilità di aggiornare le note del caso o di chiudere un caso che non sia già nello stato Chiuso o In attesa di chiusura.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Seleziona **Gestione casi** e, se richiesto, aggiungi il tuo account NSS alla Console.

   La pagina **Gestione casi** mostra i casi aperti relativi all'account NSS associato al tuo account utente della Console. Si tratta dello stesso account NSS che appare in cima alla pagina **Gestione NSS**.
3. Facoltativamente, modifica le informazioni visualizzate nella tabella:
   - In **Casi dell'organizzazione**, seleziona **Visualizza** per visualizzare tutti i casi associati alla tua azienda.
   - Modifica l'intervallo di date scegliendo un intervallo di date esatto o un intervallo di tempo diverso.
   - Filtra il contenuto delle colonne.
   - Modifica le colonne che appaiono nella tabella selezionando e quindi scegli le colonne che desideri visualizzare.
4. Gestisci un caso esistente selezionando e selezionando una delle opzioni disponibili:
   - **Visualizza caso**: visualizza i dettagli completi su un caso specifico.
   - **Aggiorna note sul caso**: fornisci ulteriori dettagli sul tuo problema o seleziona **Carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
   - **Chiudi caso**: fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.

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 NetApp Console"
- "Avviso per Cloud Volumes ONTAP"
- "Avviso per ONTAP"

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.