Guida per l'utente di Amazon S3 File Gateway

AWS Storage Gateway

Versione API 2013-06-30

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Guida per l'utente di Amazon S3 File Gateway

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l’immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cos'è Amazon S3 File Gateway 1
Come funziona S3 File Gateway 2
Guida introduttiva con Gateway di archiviazione AWS 5
Registrazione ad Amazon Web Services 5
Crea un utente IAM con privilegi di amministratore 6
Accedendo Gateway di archiviazione AWS 8
Regioni AWS che supportano Storage Gateway 8
Requisiti di configurazione di File Gate 10
Prerequisiti 10
Requisiti storage e hardware 11
Requisiti hardware per ambienti locali VMs 11
Requisiti per i tipi di EC2 istanze Amazon 11
Requisiti di storage 12
Requisiti di rete e firewall 13
Requisiti delle porte 14
Requisiti di rete e di firewall per l'appliance hardware 31
Consentire l'accesso al gateway attraverso firewall e router 34
Configurazione del gruppo di sicurezza 39
Hypervisor supportati e requisiti di hosting 39
Client NFS e SMB supportati per File Gateway 40
Operazioni del file system supportate 41
Gestione dei dischi locali 42
Determinazione della quantità di archiviazione su disco locale 42
Aggiungi spazio di archiviazione cache 43
Utilizzo dello storage temporaneo con i gateway EC2 44
Utilizzo dell'appliance hardware 46
Configurazione dell'appliance hardware 47
Installazione fisica del dispositivo hardware 49
Accesso alla console dell'apparecchiatura hardware 51
Configurazione dei parametri di rete dell'apparecchiatura hardware 52
Attivazione dell'appliance hardware 53
Creazione di un gateway sul tuo dispositivo hardware 55
Configurazione di un indirizzo IP del gateway sull'appliance hardware 56
Rimozione del software gateway dal dispositivo hardware 58

Eliminazione dell'appliance hardware ... 60
Crea il tuo gateway ... 62
Panoramica: attivazione del gateway ... 62
Configurazione di un gateway ... 62
Connect a AWS ... 62
Rivedi e attiva ... 63
Panoramica: configurazione del gateway ... 63
Panoramica: risorse di archiviazione ... 63
Crea un S3 File Gateway ... 63
Configurazione di un Amazon S3 File Gateway ... 64
Connect il tuo Amazon S3 File Gateway a AWS ... 65
Rivedi le impostazioni e attiva il tuo Amazon S3 File Gateway ... 66
Configura il tuo Amazon S3 File Gateway ... 67
Attivazione di un gateway in un VPC ... 70
Crea un endpoint VPC per Storage Gateway ... 70
Creazione di una condivisione file ... 73
Evita costi imprevisti ... 74
Crittografa gli oggetti archiviati da File Gateway ... 75
Creare una condivisione di file NFS ... 76
Crea una condivisione di file NFS con la configurazione predefinita ... 77
Crea una condivisione di file NFS con configurazione personalizzata ... 82
Creare una condivisione di file SMB ... 90
Crea una condivisione di file SMB con la configurazione predefinita ... 90
Crea una condivisione di file SMB con configurazione personalizzata ... 97
Montaggio e utilizzo della condivisione di file ... 108
Installa la condivisione di file NFS sul tuo client ... 108
Installa la tua condivisione di file SMB sul tuo client ... 110
Utilizzo di condivisioni di file su bucket con oggetti preesistenti ... 114
Metti alla prova il tuo S3 File Gateway ... 115
Gestione del tuo Amazon S3 File Gateway ... 117
Modifica le informazioni di base sul gateway ... 118
Concessione dell'accesso e delle autorizzazioni ... 119
Concessione dell'accesso a un bucket S3 ... 120
Prevenzione del problema "confused deputy" tra servizi ... 123
Utilizzo di una condivisione di file per l'accesso a più account ... 125
Eliminare una condivisione di file ... 126

Modifica delle impostazioni SMB del gateway 128
Imposta il livello di sicurezza del gateway 129
Configurare l'autenticazione di Active Directory 130
Fornisci l'accesso agli ospiti 133
Configura i gruppi locali 133
Imposta la visibilità della condivisione dei file 134
Modifica le impostazioni di condivisione di file SMB 135
Limita l'accesso alla condivisione di file SMB 137
Modificare il metodo di crittografia della condivisione dei file 138
Modifica le impostazioni di condivisione dei file NFS 139
Modifica le impostazioni predefinite dei metadati per la condivisione di file NFS 142
Limita l'accesso alla condivisione di file NFS 143
Aggiornamento della cache degli oggetti del bucket Amazon S3 143
Configurare una pianificazione di aggiornamento automatico della cache utilizzando la console Storage Gateway 144
Configura una pianificazione di aggiornamento automatico della cache utilizzando AWS Lambda una regola Amazon CloudWatch 146
Eseguire un aggiornamento manuale della cache utilizzando la console Storage Gateway .. 149
Eseguire un aggiornamento manuale della cache utilizzando l'API Storage Gateway 149
Utilizzo del blocco oggetti S3 151
Stato della condivisione dei file 151
Stato del gateway 153
Gestione della larghezza di banda 153
Modifica bandwidth-rate-limit pianificazione 154
Utilizzando il AWS SDK per Java 156
Utilizzando il AWS SDK per .NET 158
Utilizzando il AWS Tools for Windows PowerShell 161
Monitoraggio di Storage Gateway 163
Comprendere CloudWatch gli allarmi 163
Crea allarmi consigliati CloudWatch 165
Crea un CloudWatch allarme personalizzato 166
..... 168
Ottenere i registri di integrità di S3 File Gateway Gateway 168
Utilizzo dei CloudWatch parametri di Amazon 171
Ricevere notifiche sulle operazioni sui file 172
Comprendere i parametri del gateway 180

Comprensione delle metriche relative alla condivisione dei file 186
..... 190
Crea un report sulla cache 195
Gestisci i report sulla cache 198
Comprendere i report sulla cache 199
Manutenzione del gateway 202
Gestione degli aggiornamenti del gateway 202
Frequenza di aggiornamento e comportamento previsto 203
Attiva o disattiva gli aggiornamenti di manutenzione 204
Modifica la pianificazione della finestra di manutenzione del gateway 205
Applica un aggiornamento manualmente 206
Esecuzione delle attività di manutenzione utilizzando la console locale 207
Accesso alla console locale del gateway 208
Esecuzione di attività sulla console locale della macchina virtuale 211
Esecuzione di attività sulla console EC2 locale 227
Spegnimento della macchina virtuale gateway 235
Sostituzione del tuo S3 File Gateway esistente con una nuova istanza 235
Metodo 1: migra il disco di cache e l'ID del gateway su un'istanza sostitutiva 238
Metodo 2: istanza sostitutiva con disco di cache vuoto e nuovo Gateway ID 241
Eliminazione del gateway e rimozione delle risorse 243
Eliminazione del gateway tramite la console Storage Gateway 243
Prestazioni e ottimizzazione 246
..... 246
Prestazioni di S3 File Gateway su client Linux 247
Prestazioni di File Gateway sui client Windows 249
Indicazioni sulle prestazioni per gateway con più condivisioni di file 250
Massimizzazione del throughput di S3 File Gateway 253
Implementa il gateway nella stessa posizione dei tuoi client 253
Riduci i colli di bottiglia causati dai dischi lenti 254
Modifica l'allocazione delle risorse delle macchine virtuali per CPU, RAM e dischi cache 254
Regola il livello di sicurezza delle PMI 256
Utilizza più thread e client per parallelizzare le operazioni di scrittura 257
Disattiva l'aggiornamento automatico della cache 259
Aumenta il numero di thread di caricamento di Amazon S3 260
Aumenta le impostazioni di timeout SMB 260
Attiva il blocco opportunistico per le applicazioni compatibili 261

Regola la capacità del gateway in base alla dimensione del set di file di lavoro 261
Implementa più gateway per carichi di lavoro più grandi 262
Ottimizzazione di S3 File Gateway per i backup dei database SQL Server 263
Implementa il gateway nella stessa posizione dei server SQL 264
Riduci i colli di bottiglia causati dai dischi lenti 264
Regola l'allocazione delle risorse della macchina virtuale S3 File Gateway per CPU, RAM e dischi cache 265
Migliora la produttività dei client SMB regolando il livello di sicurezza del tuo S3 File Gateway 266
Migliora la produttività dei client SMB suddividendo i backup SQL in più file 267
Previeni errori di copia di file di grandi dimensioni aumentando le impostazioni di timeout SMB 268
Aumenta il numero di thread di caricamento di Amazon S3 269
Disattiva l'aggiornamento automatico della cache 269
Implementa più gateway per supportare il carico di lavoro 270
Risorse aggiuntive per i carichi di lavoro di backup del database 270
Sicurezza 272
Protezione dei dati 272
Crittografia dei dati 273
Gestione dell’identità e degli accessi 274
Destinatari 275
Autenticazione con identità 275
Gestione dell’accesso tramite policy 276
Come funziona AWS Storage Gateway con IAM 278
Esempi di policy basate su identità 284
risoluzione dei problemi 287
Utilizzo dei tag per controllare l'accesso alle risorse 289
Utilizzo ACLs per l'accesso alla condivisione di file SMB 292
Convalida della conformità 296
Resilienza 297
Sicurezza dell’infrastruttura 297
AWS Migliori pratiche di sicurezza 298
Registrazione di log e monitoraggio 298
Informazioni sullo Storage Gateway in CloudTrail 299
Informazioni sulle voci dei file di registro di Storage Gateway 300
risoluzione dei problemi 303

Risoluzione dei problemi: problemi relativi al gateway offline 304
Controlla il firewall o il proxy associato 304
Verifica la presenza di un'ispezione continua tramite SSL o deep packet del traffico del tuo gateway 304
Controlla la metrica IOWait Percentuale dopo un riavvio o un aggiornamento del software .. 304
Verificare la presenza di un'interruzione dell'alimentazione o di un guasto hardware sull'host dell'hypervisor 305
Verifica la presenza di problemi con un disco di cache associato 305
Risoluzione dei problemi: problemi relativi ad Active Directory 306
Verifica che il gateway possa raggiungere il controller di dominio eseguendo un test nping . 306
Verifica le opzioni DHCP impostate per il VPC della tua istanza Amazon gateway EC2 307
Verifica che il gateway sia in grado di risolvere il dominio eseguendo una query dig 307
Controlla le impostazioni e i ruoli del controller di dominio 308
Verifica che il gateway sia aggiunto al controller di dominio più vicino 308
Verifica che Active Directory crei nuovi oggetti informatici nell'unità organizzativa (OU) predefinita 309
Controlla i registri degli eventi del controller di dominio 309
Risoluzione dei problemi: problemi di attivazione del gateway 310
Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico 310
Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint Amazon VPC 313
Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico e nello stesso VPC è presente un endpoint VPC Storage Gateway 317
Risoluzione dei problemi: problemi relativi al gateway locale 318
Risoluzione dei problemi: aprire le porte NFS 322
Attivazione dell' Supporto accesso per facilitare la risoluzione dei problemi del gateway 323
Risoluzione dei problemi: problemi di configurazione di Microsoft Hyper-V 324
Risoluzione dei problemi: problemi relativi al EC2 gateway Amazon 328
Dopo qualche secondo, il gateway ancora non si attiva 328
Impossibile trovare l'istanza del EC2 gateway nell'elenco delle istanze 329
Connect al EC2 gateway Amazon tramite la console seriale 329
Attivazione dell' Supporto accesso per facilitare la risoluzione dei problemi relativi al gateway 329
Risoluzione dei problemi: problemi relativi alle apparecchiature hardware 331
Come determinare l'indirizzo IP del servizio 332
Come si esegue una reimpostazione ai valori di fabbrica 332
Come eseguire il riavvio a distanza 332

Come ottenere il supporto Dell iDRAC 332
Come trovare il numero di serie dell'appliance hardware 333
Come ottenere supporto per il dispositivo hardware 333
Risoluzione dei problemi: problemi relativi a File Gateway 334
Errore: 1344 (0x00000540) 334
Errore: GatewayClockOutOfSync 335
Errore: InaccessibleStorageClass 335
Errore: InvalidObjectState 336
Errore: ObjectMissing 336
Errore: RoleTrustRelationshipInvalid 337
Errore: S3 AccessDenied 337
Errore: DroppedNotifications 338
Notifica: HardReboot 339
Notifica: riavvio 339
Risoluzione dei problemi: aprire le porte NFS 322
Risoluzione dei problemi relativi alle metriche CloudWatch 341
Risoluzione dei problemi: problemi relativi alla condivisione dei file 343
La condivisione del file è bloccata nello stato CREATING 344
Impossibile creare una condivisione di file 345
Le condivisioni di file SMB non consentono più metodi di accesso diversi 345
Le condivisioni di file multiple non possono scrivere sul bucket S3 mappato 346
Notifica per il gruppo di log eliminato quando si utilizzano i log di controllo 346
Impossibile caricare file nel bucket S3 346
Impossibile modificare la crittografia predefinita in SSE-KMS 346
Le modifiche apportate direttamente in un bucket S3 con il controllo delle versioni degli oggetti attivato possono influire su ciò che vedi nella condivisione di file 347
Quando si scrive su un bucket S3 con il controllo delle versioni attivato, Amazon S3 File Gateway può creare più versioni di oggetti Amazon S3 348
Le modifiche a un bucket S3 non si riflettono in Storage Gateway 349
Le autorizzazioni ACL non funzionano come previsto 350
Le prestazioni del gateway sono diminuite dopo un'operazione ricorsiva 350
Notifiche di stato della disponibilità elevata 351
Risoluzione dei problemi: problemi di elevata disponibilità 351
Notifiche di stato 351
Parametri 353
Best practice 354

Recupero dei dati ... 354
Ripristino da un arresto imprevisto della macchina virtuale ... 355
Ripristino dei dati da un disco della cache malfunzionante ... 355
Ripristino dei dati da un data center inaccessibile ... 355
Gestione dei caricamenti in più parti ... 356
Decompressione di file compressi ... 356
Copia di dati da Windows Server ... 357
Dimensionamento dei dischi di cache ... 357
Condivisioni di file e bucket multipli ... 358
Pulisci le risorse non necessarie ... 359
Risorse aggiuntive ... 360
Configurazione dell'host ... 361
Implementa un EC2 host Amazon predefinito per File Gateway ... 361
Implementa un EC2 host Amazon personalizzato per File Gateway ... 364
Modifica le opzioni dei metadati delle EC2 istanze Amazon ... 368
Sincronizza l'ora della macchina virtuale con l'ora dell'host KVM Hyper-V o Linux ... 368
Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware ... 369
Configurazione degli adattatori di rete per il gateway ... 371
Utilizzo di Storage Gateway con VMware HA ... 374
Ottenere la chiave di attivazione ... 378
Linux (curl) ... 379
Linux (bash/zsh) ... 381
Microsoft Windows PowerShell ... 382
Utilizzo della console locale ... 382
Supporto per gli attributi di file ... 384
Usando Direct Connect ... 385
Autorizzazioni Active Directory ... 385
Ottenere l'indirizzo IP del gateway ... 386
Ottenere un indirizzo IP da un EC2 host Amazon ... 387
IPv6 supporto ... 388
Comprendere le risorse e le risorse IDs ... 388
Lavorare con Resource IDs ... 388
Tagging delle risorse ... 389
Lavorare con i tag ... 390
Componenti open source ... 391
Componenti open source per Storage Gateway ... 392

Componenti open source per Amazon S3 File Gateway 392
Quote 392
Quote per le condivisioni di file 392
Dimensioni disco locale consigliate per il gateway 395
Utilizzo delle classi di archiviazione 396
Utilizzo di classi di storage con un File Gateway 396
Utilizzo della classe di archiviazione GLACIER con File Gateway 402
Utilizzo dei driver Kubernetes CSI 402
Lavorare con i driver CSI SMB 403
Utilizzo dei driver NFS CSI 407
Modulo Terraform 411
Documentazione di riferimento delle API 413
Intestazioni obbligatorie delle richieste 413
Firmare le richieste 416
Esempio di calcolo di firma 417
Risposte agli errori 418
Eccezioni 419
Codici di errore delle operazioni 421
Risposte agli errori 442
Azioni 444
Cronologia dei documenti 445
Aggiornamenti precedenti 462
Note di rilascio 466
..... cdlxxxix

Cos'è Amazon S3 File Gateway

Amazon S3 File Gateway — Amazon S3 File Gateway supporta un'interfaccia di file in Amazon Simple Storage Service (Amazon S3) e combina un servizio e un'appliance software virtuale. Utilizzando questa combinazione, puoi archiviare e recuperare oggetti in Amazon S3 utilizzando protocolli di file standard del settore come Network File System (NFS) e Server Message Block (SMB). Puoi implementare il gateway nel tuo ambiente locale come macchina virtuale (VM) in esecuzione su VMware ESXi Microsoft Hyper-V o macchina virtuale basata su Linux Kernel (KVM) o come appliance hardware ordinata dal tuo rivenditore preferito. Puoi anche implementare la macchina virtuale Storage Gateway nel VMware cloud o come AMI in Amazon. AWS EC2 Il gateway fornisce l'accesso agli oggetti in S3 come punti di montaggio per file o condivisioni di file. Con un S3 File Gateway, puoi fare quanto segue:

- Archiviare e recuperare i file direttamente tramite il protocollo NFS versione 3 o 4.1.
- Archiviare e recuperare i file direttamente tramite il protocollo file system SMB versione 2 e 3.
- Puoi accedere ai tuoi dati direttamente in Amazon S3 da qualsiasi applicazione o AWS servizio cloud.
- Puoi gestire i tuoi dati S3 utilizzando politiche del ciclo di vita, replica tra regioni e controllo delle versioni. Puoi pensare a S3 File Gateway come a un montaggio di file system su Amazon S3.

Un S3 File Gateway semplifica lo storage dei file in Amazon S3, si integra con le applicazioni esistenti tramite protocolli di file system standard del settore e fornisce un'alternativa economica allo storage locale. Fornisce inoltre accesso a bassa latenza ai dati tramite caching locale trasparente. Un S3 File Gateway gestisce il trasferimento dei dati da e verso AWS, protegge le applicazioni dalla congestione della rete, ottimizza e trasmette i dati in parallelo e gestisce il consumo di larghezza di banda.

S3 File Gateway si integra con altri servizi, ad esempio: AWS

- Gestione comune degli accessi tramite AWS Identity and Access Management (IAM)
- Crittografia tramite AWS Key Management Service (AWS KMS)
- Monitoraggio tramite Amazon CloudWatch (CloudWatch)
- Verifica utilizzando AWS CloudTrail (CloudTrail)
- Operazioni che utilizzano Console di gestione AWS and AWS Command Line Interface (AWS CLI)
- Gestione di costi e fatturazione

Nella documentazione seguente, troverai la sezione Nozioni di base che contiene le informazioni di configurazione comuni a tutti i gateway, nonché sezioni sulla configurazione specifica per gateway. La sezione Nozioni di base illustra come distribuire, attivare e configurare lo storage per un gateway. La sezione sulla gestione illustra come gestire il gateway e le risorse:

- fornisce istruzioni su come creare e utilizzare un S3 File Gateway. Ti mostra come creare una condivisione di file, mappare l'unità su un bucket Amazon S3 e caricare file e cartelle su Amazon S3.

- descrive come eseguire le attività di gestione per tutti i tipi e le risorse di gateway.

In questa guida, scoprirai principalmente come utilizzare le operazioni dei gateway tramite la Console di gestione AWS. Se si desidera eseguire queste operazioni a livello di codice, consultare AWS Io Storage Gateway API Reference.

Come funziona Amazon S3 File Gateway

Per utilizzare un S3 File Gateway, iniziate scaricando un'immagine VM per il gateway. È quindi possibile attivare il gateway da Console di gestione AWS o tramite l'API Storage Gateway. Puoi anche creare un S3 File Gateway utilizzando un' EC2 immagine Amazon.

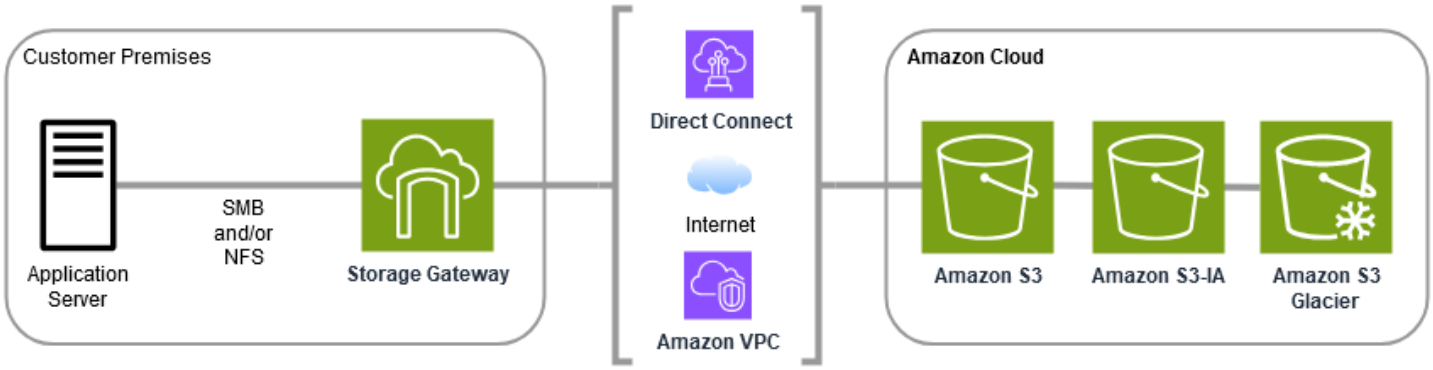
Dopo l'attivazione di S3 File Gateway, crei e configuri la condivisione di file e la associ al tuo bucket Amazon Simple Storage Service (Amazon S3). In questo modo la condivisione è accessibile ai client che utilizzano il protocollo Network File System (NFS) o Server Message Block (SMB). I file scritti in una condivisione di file diventano oggetti in Amazon S3, con il percorso come chiave. Esiste una one-to-one mappatura tra file e oggetti e il gateway aggiorna in modo asincrono gli oggetti in Amazon S3 man mano che modifichi i file. Gli oggetti esistenti nel bucket Amazon S3 vengono visualizzati come file nel file system e la chiave diventa il percorso. Gli oggetti sono crittografati con Amazon S3, chiavi di crittografia lato server (SSE-S3). Tutti i trasferimenti di dati vengono eseguiti tramite HTTPS.

Quando si inviano richieste di caricamento di dati HTTPS ad Amazon S3, File Gateway compila l'MD5 intestazione Content- con il MD5 checksum dei dati caricati. L'uso di questa intestazione fa sì che Amazon S3 restituisca un errore in caso di mancata corrispondenza tra MD5 il checksum calcolato da Amazon S3 e il valore ricevuto da File Gateway. Se viene restituito un errore di questo tipo, File Gateway invia nuovamente la richiesta.

Il servizio ottimizza il trasferimento di dati tra il gateway e AWS utilizzando caricamenti paralleli multiparte o download per intervallo di byte, per utilizzare meglio la larghezza di banda disponibile. La

cache locale viene gestita per fornire un accesso a bassa latenza ai dati a cui si accede di recente e ridurre i costi di uscita dei dati. CloudWatch le metriche forniscono informazioni sull'uso delle risorse sulla macchina virtuale e sul trasferimento dei dati da e verso. AWS CloudTrail tiene traccia di tutte le chiamate API.

Con lo storage S3 File Gateway, puoi eseguire attività come l'acquisizione di carichi di lavoro cloud su Amazon S3, l'esecuzione di backup e archiviazione, il tiering e la migrazione dei dati di storage sul cloud. AWS Il diagramma seguente fornisce una panoramica dell'implementazione dello storage di file per Storage Gateway.



S3 File Gateway converte i file in oggetti S3 durante il caricamento di file su Amazon S3. L'interazione tra le operazioni sui file eseguite sulle condivisioni di file su S3 File Gateway e gli oggetti S3 richiede un'attenta considerazione di alcune operazioni durante la conversione tra file e oggetti.

Le operazioni comuni sui file modificano i metadati dei file, il che comporta l'eliminazione dell'oggetto S3 corrente e la creazione di un nuovo oggetto S3. La tabella seguente mostra esempi di operazioni sui file e l'impatto sugli oggetti S3.

Operazione sui file	Impatto sugli oggetti S3	Implicazione della classe di archiviazione
Rinomina file	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file	Potrebbero essere applicati costi di cancellazione anticipat a e costi di recupero
Rinomina cartella	Sostituisce tutti gli oggetti S3 esistenti e crea nuovi oggetti S3 per ogni cartella e file nella struttura delle cartelle	Potrebbero essere applicati costi di cancellazione anticipat a e costi di recupero

Operazione sui file	Impatto sugli oggetti S3	Implicazione della classe di archiviazione
Modifica le autorizzazioni file/folder	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file o cartella	Potrebbero essere applicati costi di cancellazione anticipat a e costi di recupero
Cambia proprietà file/folder	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file o cartella	Potrebbero essere applicati costi di cancellazione anticipat a e costi di recupero
Aggiungi a un file	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file	Potrebbero essere applicati costi di cancellazione anticipat a e costi di recupero

Quando un file viene scritto su S3 File Gateway da un client NFS o SMB, File Gateway carica i dati del file su Amazon S3 seguiti dai relativi metadati (proprietà, timestamp, ecc.). Il caricamento dei dati del file crea un oggetto S3 e il caricamento dei metadati per il file aggiorna i metadati per l'oggetto S3. Questo processo crea un'altra versione dell'oggetto, ottenendo due versioni di un oggetto. Se S3 Versioning è attivato, entrambe le versioni verranno archiviate.

Quando un file viene modificato in S3 File Gateway da un client NFS o SMB dopo che è stato caricato su Amazon S3, S3 File Gateway carica i dati nuovi o modificati anziché caricare l'intero file. La modifica del file comporta la creazione di una nuova versione dell'oggetto S3.

Quando S3 File Gateway carica file di grandi dimensioni, potrebbe essere necessario caricare porzioni più piccole del file prima che il client abbia finito di scrivere su S3 File Gateway. Alcuni motivi includono la liberazione di spazio nella cache o un'elevata velocità di scrittura su una condivisione di file. Ciò può comportare la creazione di più versioni di un oggetto nel bucket S3.

È necessario monitorare il bucket S3 per determinare quante versioni di un oggetto esistono prima di configurare le politiche del ciclo di vita per spostare gli oggetti in classi di storage diverse. È necessario configurare la scadenza del ciclo di vita per le versioni precedenti per ridurre al minimo il numero di versioni di un oggetto nel bucket S3. L'uso della replica Same-Region (SRR) o della replica Cross-Region (CRR) tra i bucket S3 aumenterà lo storage utilizzato.

Guida introduttiva con Gateway di archiviazione AWS

Questa sezione fornisce istruzioni per iniziare AWS. È necessario disporre di un AWS account prima di poter iniziare a utilizzare Gateway di archiviazione AWS. Puoi utilizzare un AWS account esistente o registrarne uno nuovo. È inoltre necessario che nel proprio AWS account sia presente un utente IAM che appartenga a un gruppo con le autorizzazioni amministrative necessarie per eseguire le attività di Storage Gateway. Gli utenti con i privilegi appropriati possono accedere alla console Storage Gateway e all'API Storage Gateway per eseguire attività di implementazione, configurazione e manutenzione del gateway. Se sei un utente alle prime armi, ti consigliamo di consultare le sezioni AWS Regioni supportate e Requisiti di configurazione del File Gateway prima di iniziare a utilizzare Storage Gateway.

Questa sezione contiene i seguenti argomenti, che forniscono informazioni aggiuntive su come iniziare a Gateway di archiviazione AWS:

Argomenti

- Registrazione ad Amazon Web Services- Scopri come registrarti AWS e creare un AWS account.
- Crea un utente IAM con privilegi di amministratore- Scopri come creare un utente IAM con privilegi amministrativi per il tuo AWS account.
- Accedendo Gateway di archiviazione AWS- Scopri come accedere Gateway di archiviazione AWS tramite la console Storage Gateway o utilizzando programmaticamente il. AWS SDKs
- Regioni AWS che supportano Storage Gateway- Scopri quali AWS regioni puoi utilizzare per archiviare i tuoi dati quando attivi il gateway in Storage Gateway.

Registrazione ad Amazon Web Services

An Account AWS è un requisito fondamentale per accedere ai AWS servizi. Your Account AWS è il contenitore di base per tutte le AWS risorse che crei come AWS utente. Il tuo Account AWS è anche il limite di sicurezza di base per AWS le tue risorse. Tutte le risorse che crei nel tuo account sono disponibili per gli utenti che dispongono delle credenziali per l'account. Prima di poter iniziare a utilizzare Gateway di archiviazione AWS, devi registrarti per un Account AWS.

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire le attività che richiedono l'accesso di un utente root.

Ti consigliamo inoltre di richiedere agli utenti di utilizzare credenziali temporanee per l'accesso AWS. Per fornire credenziali temporanee, puoi utilizzare la federazione e un provider di identità, come AWS IAM Identity Center. Se la tua azienda utilizza già un provider di identità, puoi utilizzarlo con la federazione per semplificare il modo in cui fornisci l'accesso alle risorse del tuo AWS account.

Crea un utente IAM con privilegi di amministratore

Dopo aver creato l' AWS account, segui i passaggi seguenti per creare un utente AWS Identity and Access Management (IAM) per te stesso, quindi aggiungi quell'utente a un gruppo con autorizzazioni amministrative. Per ulteriori informazioni sull'utilizzo del AWS Identity and Access Management servizio per controllare l'accesso alle risorse di Storage Gateway, vedereGestione delle identità e degli accessi per AWS Storage Gateway.

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center (Consigliato)	Usa credenziali a breve termine per accedere a AWS. Ciò è in linea con le best practice per la sicurezza. Per informazioni sulle best practice, consulta Best practice per la sicurezza in IAM nella Guida per l'utente di IAM.	Segui le istruzioni riportate in Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .	Configurare l'accesso programmatico configurando l'uso AWS IAM Identity Center nella Guida AWS CLI per l'AWS Command Line Interface utente.
In IAM (Non consigliato)	Usa credenziali a lungo termine per accedere a AWS.	Segui le istruzioni in Creare un utente IAM per l'accesso di emergenza nella Guida per l'utente di IAM.	Configura l'accesso programmatico seguendo quanto riportato in Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Warning

Gli utenti IAM dispongono di credenziali a lungo termine che presentano un rischio per la sicurezza. Per ridurre questo rischio, si consiglia di fornire a questi utenti solo le autorizzazioni necessarie per eseguire l'attività e di rimuoverli quando non sono più necessari.

Accedendo Gateway di archiviazione AWS

Per semplicità e facilità d'uso, questa guida si concentra sull'esecuzione di attività utilizzando l'interfaccia Web della console Storage Gateway. È possibile accedere alla console Storage Gateway tramite il browser Web all'indirizzo:https://console.aws.amazon.com/storagegateway/home/.

Se si preferisce un approccio programmatico, è possibile utilizzare l'API (Gateway di archiviazione AWS Application Programming Interface) o l'interfaccia a riga di comando (CLI) per configurare e gestire le risorse nell'implementazione di Storage Gateway. Per ulteriori informazioni sulle azioni, i tipi di dati e la sintassi richiesta per l'API Storage Gateway, consulta lo Storage Gateway API Reference. Per ulteriori informazioni sulla CLI di Storage Gateway, vedere il CLI Command Reference AWS .

È inoltre possibile utilizzarlo AWS SDKs per sviluppare applicazioni che interagiscono con Storage Gateway. AWS SDKs Per Java, .NET e PHP racchiudono l'API Storage Gateway sottostante per semplificare le attività di programmazione. Per informazioni sul download delle librerie SDK, consulta il AWS Developer Center.

Per informazioni sui prezzi, consultare Prezzi di Gateway di archiviazione AWS.

Regioni AWS che supportano Storage Gateway

An Regione AWS è una posizione fisica nel mondo in cui sono AWS presenti più zone di disponibilità. Le zone di disponibilità sono costituite da uno o più data AWS center discreti, ciascuno con alimentazione, rete e connettività ridondanti, ospitati in strutture separate. Ciò significa che ciascuna Regione AWS è fisicamente isolata e indipendente dalle altre regioni. Le regioni forniscono la tolleranza ai guasti, la stabilità e la resilienza e possono anche ridurre la latenza. Le risorse create in una regione non esistono in nessun'altra regione a meno che non si utilizzi esplicitamente una funzionalità di replica offerta da un AWS servizio. Ad esempio, Amazon S3 e Amazon EC2 supportano la replica tra regioni. Alcuni servizi, ad esempio AWS Identity and Access Management, non dispongono di risorse regionali. Puoi lanciare AWS risorse in sedi che soddisfano i tuoi requisiti aziendali. Ad esempio, potresti voler avviare EC2 istanze Amazon per ospitare i tuoi Gateway di archiviazione AWS dispositivi Regione AWS in Europa per essere più vicino ai tuoi utenti europei o per soddisfare i requisiti legali. L'utente Account AWS determina quali delle regioni supportate da un servizio specifico sono disponibili per l'uso.

- Storage Gateway: per AWS le regioni supportate e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere Gateway di archiviazione AWS endpoint e quote nel. Riferimenti generali di AWS

- Storage Gateway Hardware Appliance: per le regioni supportate che è possibile utilizzare con l'appliance hardware, vedere Gateway di archiviazione AWS Hardware Appliance Regions nel. Riferimenti generali di AWS

Requisiti di configurazione di File Gate

Salvo diversa indicazione, i seguenti requisiti sono comuni a tutti i tipi di File Gateway in Gateway di archiviazione AWS. La configurazione deve soddisfare i requisiti indicati in questa sezione. Esamina i requisiti applicabili alla configurazione del gateway prima di implementarlo.

Argomenti

- Prerequisiti
- Requisiti storage e hardware
- Requisiti di rete e firewall
- Hypervisor supportati e requisiti di hosting
- Client NFS e SMB supportati per File Gateway
- Operazioni di file system supportate per File Gateway
- Gestione dei dischi locali per il gateway

Prerequisiti

Prima di configurare Amazon S3 File Gateway (S3 File Gateway), devi soddisfare i seguenti prerequisiti:

- Configurare Microsoft Active Directory (AD) e creare un account del servizio Active Directory con le autorizzazioni necessarie. Per ulteriori informazioni, vedere Requisiti di autorizzazione dell'account del servizio Active Directory Requisiti di autorizzazione dell'.
- Verificare che vi sia una larghezza di banda di rete sufficiente tra il gateway e AWS. È necessario un minimo di 100 Mbps per scaricare, attivare e aggiornare correttamente il gateway.
- Configura la connessione che desideri utilizzare per il traffico di rete tra AWS e l'ambiente locale in cui stai implementando il gateway. Puoi connetterti utilizzando la rete Internet pubblica, una rete privata, una VPN o. Direct Connect Se desideri che il tuo gateway comunichi AWS tramite una connessione privata a un Amazon Virtual Private Cloud, configura Amazon VPC prima di configurare il gateway.
- Assicurati che il gateway sia in grado di risolvere il nome del tuo controller di dominio Active Directory. È possibile utilizzare DHCP nel dominio Active Directory per gestire la risoluzione o specificare manualmente un server DNS dal menu delle impostazioni di configurazione di rete nella console locale del gateway.

Requisiti storage e hardware

Le seguenti sezioni forniscono informazioni sulle configurazioni hardware e di storage minime richieste per il gateway e sulla quantità minima di spazio su disco da allocare per lo storage richiesto.

Per informazioni sulle procedure consigliate per le prestazioni di File Gateway, vedere.

Requisiti hardware per ambienti locali VMs

Quando distribuisci il gateway in locale, assicurati che l'hardware sottostante su cui distribuisci la macchina virtuale (VM) gateway possa dedicare le seguenti risorse minime:

- Quattro processori virtuali assegnati alla macchina virtuale
- 16 GiB di RAM riservata per i gateway di file
- 80 GiB di spazio su disco per l'installazione di immagini VM e dati di sistema

Per ulteriori informazioni, consulta Massimizzazione del throughput di S3 File Gateway. Per ulteriori informazioni su come l'hardware influisce sulle prestazioni della macchina virtuale del gateway, vedere Quote per le condivisioni di file.

Requisiti per i tipi di EC2 istanze Amazon

Quando distribuisci il gateway su Amazon Elastic Compute Cloud EC2 (Amazon), la dimensione dell'istanza deve essere almeno **`xlarge`**per il funzionamento del gateway. Tuttavia, per la famiglia di istanze ottimizzate per il calcolo, la dimensione deve essere almeno. **`2xlarge`**

> **Note**
>
> L'AMI Storage Gateway è compatibile solo con le istanze basate su x86 che utilizzano processori Intel o AMD. Le istanze basate su ARM che utilizzano processori Graviton non sono supportate.

Utilizza uno dei seguenti tipi di istanza consigliati per il tuo tipo di gateway.

Consigliato per i tipi di File Gateway

- Famiglia di istanze per uso generico: tipo di istanza m5, m6 o m7. Scegli la dimensione dell'istanza xlarge o superiore per soddisfare i requisiti del processore e della RAM dello Storage Gateway.

- Famiglia di istanze ottimizzate per l'elaborazione: tipi di istanze c5, c6 o c7. Scegli la dimensione dell'istanza 2xlarge o superiore per soddisfare i requisiti del processore Storage Gateway e della RAM.
- Famiglia di istanze ottimizzate per la memoria: tipi di istanze r5, r6 o r7. Scegli la dimensione dell'istanza xlarge o superiore per soddisfare i requisiti del processore e della RAM dello Storage Gateway.
- Famiglia di istanze ottimizzate per lo storage: tipi di istanze i3, i4 o i7. Scegli la dimensione dell'istanza xlarge o superiore per soddisfare i requisiti del processore e della RAM dello Storage Gateway.

> **Note**
>
> Quando avvii il gateway in Amazon EC2 e il tipo di istanza scelto supporta lo storage temporaneo, i dischi vengono elencati automaticamente. Per ulteriori informazioni sullo storage di EC2 istanze Amazon, consulta Instance Storage nella Amazon EC2 User Guide. Le scritture delle applicazioni vengono archiviate nella cache in modo sincrono e quindi caricate in modo asincrono su uno storage durevole in Amazon S3. Se lo storage temporaneo viene perso perché un'istanza si interrompe prima del completamento del caricamento, i dati che risiedono ancora nella cache e non sono ancora stati scritti su Amazon Simple Storage Service (Amazon S3) possono andare persi. Prima di interrompere l'istanza che ospita il gateway, assicurati che la metrica sia corretta. `CachePercentDirty` CloudWatch `0` Per informazioni sullo storage temporaneo, consulta Utilizzo dello storage temporaneo con i gateway EC2 . Per informazioni sulle metriche di monitoraggio per lo Storage Gateway, vedere.
> Se hai più di 5 milioni di oggetti nel tuo bucket S3 e utilizzi un volume EBS gp2, è necessario un volume EBS root minimo di 350 GiB per prestazioni accettabili del gateway durante l'avvio. Le istanze Amazon EC2 File Gateway appena create utilizzano per impostazione predefinita i volumi root gp3, che non hanno questo requisito. Per informazioni su come aumentare la dimensione del volume, consulta Modificare un volume EBS utilizzando volumi elastici (console).

Requisiti di storage

Oltre a 80 GiB di spazio su disco per la macchina virtuale, sono necessari anche dischi aggiuntivi per il gateway.

Tipo di gateway	Cache (minimo)	Cache (massima)			
Gateway file	150 GiB	64 TiB			

> **Note**
>
> È possibile configurare una o più unità locali per la cache, fino alla capacità massima. Quando si aggiunge la cache a un gateway esistente, è importante creare nuovi dischi nell'host (hypervisor o istanza Amazon EC2). Non modificare le dimensioni dei dischi esistenti se i dischi sono stati precedentemente allocati come cache.

Per informazioni sulle quote del gateway, consulta Quote per le condivisioni di file.

Requisiti di rete e firewall

Il gateway richiede accesso a internet, reti locali, server DNS (Domain Name Service), firewall, router ecc.

I requisiti di larghezza di banda della rete variano in base alla quantità di dati caricati e scaricati dal gateway. È necessario un minimo di 100 Mbps per scaricare, attivare e aggiornare correttamente il gateway. I modelli di trasferimento dei dati determineranno la larghezza di banda necessaria per supportare il carico di lavoro.

Di seguito, puoi trovare ulteriori informazioni sulle porte e sulle modalità per consentire l'accesso tramite firewall e router.

> **Note**
>
> In alcuni casi, potresti implementare il tuo gateway su Amazon EC2 o utilizzare altri tipi di distribuzione (inclusa quella locale) con politiche di sicurezza di rete che limitano gli intervalli di indirizzi AWS IP. In questi casi, il gateway potrebbe riscontrare problemi di connettività del servizio quando i valori dell'intervallo AWS IP cambiano. I valori dell'intervallo di indirizzi AWS IP che devi utilizzare si trovano nel sottoinsieme di servizi Amazon per la AWS regione in cui attivi il gateway. Per i valori correnti dell'intervallo IP, consulta Intervalli di indirizzi IP AWS nella Riferimenti generali di AWS.

Argomenti

- Requisiti delle porte
- Requisiti di rete e di firewall per l'appliance hardware Storage Gateway
- Consentire Gateway di archiviazione AWS l'accesso tramite firewall e router
- Configurazione dei gruppi di sicurezza per la tua istanza Amazon EC2 gateway

Requisiti delle porte

S3 File Gateway richiede l'autorizzazione di porte specifiche attraverso la sicurezza di rete per una distribuzione e un funzionamento corretti. Alcune porte sono necessarie per tutti i gateway, mentre altre sono necessarie solo per configurazioni specifiche, ad esempio per la connessione a client NFS o SMB, endpoint VPC o Microsoft Active Directory.

Per S3 File Gateway, è necessario utilizzare Microsoft Active Directory solo quando si desidera consentire agli utenti del dominio di accedere a una condivisione di file Server Message Block (SMB). Puoi aggiungere il tuo File Gateway a qualsiasi dominio Microsoft Windows valido (risolvibile tramite DNS).

Puoi anche Directory Service utilizzarlo per crearne uno AWS Managed Microsoft ADin Amazon Web Services Cloud. Per la maggior parte delle AWS Managed Microsoft AD implementazioni, è necessario configurare il servizio DHCP (Dynamic Host Configuration Protocol) per il VPC. Per informazioni sulla creazione di un set di opzioni DHCP, vedere Create a DHCP options set nella Administration Guide.AWS Directory Service

La tabella seguente elenca le porte necessarie e descrive i requisiti condizionali nella colonna Note.

Requisiti di porta per S3 File Gateway File Gateway

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Browser	Browser	Macchina virtuale Storage Gateway	TCP/ HTTP	80	✓	✓	✓	Utilizzato dai sistemi locali per ottenere

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								la chiave di attivazione dello Storage Gateway. La porta 80 viene usata solo durante l'attivazione di un'appliance Storage Gateway. Per una macchina virtuale Storage Gateway la porta 80 non deve essere accessibile pubblicamente. Il livello di accesso

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								richiesto alla porta 80 dipende dalla configurazione di rete. Se si attiva il gateway dalla Storage Gateway Management Console, l'host da cui ci si connette alla console deve avere accesso alla porta 80 del gateway.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Browser	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓	AWS Console di gestione (tutte le altre operazioni)
DNS	Macchina virtuale Storage Gateway	Server DNS (Domain Name Service)	DNS TCP E UDP	53	✓	✓	✓	Utilizzato per la comunicazione tra una macchina virtuale Storage Gateway e il server DNS per la risoluzione dei nomi IP.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
NTP	Macchina virtuale Storage Gateway	Server NTP (Network Time Protocol)	TCP E UDP NTP	123	✓	✓	✓	Utilizzato dai sistemi locali per sincronizzare l'ora della macchina virtuale con l'ora dell'host. Una macchina virtuale Storage Gateway è configurata in modo che possa utilizzare i seguenti server NTP: • 0.amazon.pool.ntp.org

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								• 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org **Note** Non richiesto per i gateway ospitati su Amazon EC2.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Storage Gateway	Macchina virtuale Storage Gateway	Supporto Endpoint	TCP/ SSH	22	✓	✓	✓	Consente di accedere Supporto al gateway per aiutarti a risolvere i problemi relativi al gateway. Non è necessario che la porta sia aperta per il normale funzionamento del gateway, tuttavia è necessario per la risoluzione dei problemi.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								Per un elenco degli endpoint di supporto, consulta Supporto endpoints.
Storage Gateway	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓	Controllo della gestione
Amazon CloudFront	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓	Per l'attivazione
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓*	Controllo della gestione *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1026		✓	✓*	Endpoint del Control Plane *Richiesto solo quando si utilizzano gli endpoint VPC
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1027		✓	✓*	Anon Control Plane (per l'attivazione) *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1028		✓	✓*	Endpoint proxy *Richiesto solo quando si utilizzano gli endpoint VPC
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1031		✓	✓*	Piano dei dati *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	2222		✓	✓*	Canale di supporto SSH per VPCe *Necessario solo per l'apertura del canale di supporto quando si utilizzano gli endpoint VPC
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓*	Controllo della gestione *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Client della condivisione file	Client SMB	Macchina virtuale Storage Gateway	TCP o UDP SMBv3	445	✓	✓	✓*	Servizio di sessione di trasferimento dati per la condivisione di file. Sostituisce le porte 137-139 per Microsoft Windows NT e versioni successive. *Richiesto solo per SMB.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	UDP per NetBIOS	137	✓	✓	✓*	Servizio di denominazione *Richiesto SMBv1 solo per.
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	UDP per NetBIOS	138	✓	✓	✓*	Servizio datagramma *Richiesto solo per SMBv1 .
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	TCP E UDP LDAP	389	✓	✓	✓*	Connessione client Directory System Agent (DSA) *Richiesto solo per SMB.

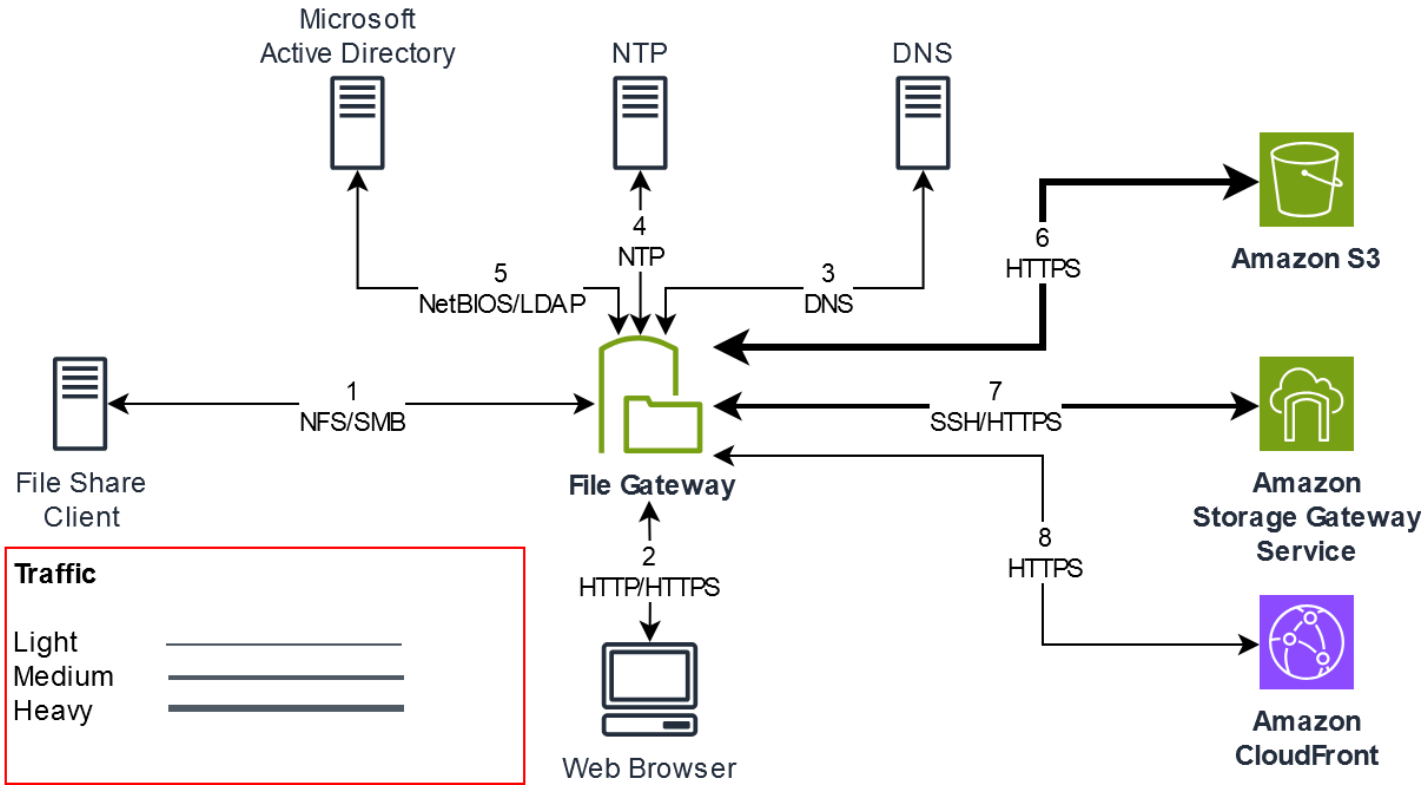
Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	Kerberos TCP e UDP	88	✓	✓	✓*	Kerberos *Richiesto solo per SMB.
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	TCP Distributed Computing Environment/End Point Mapper (DCE/EMAP)	135	✓	✓	✓*	RPC *Richiesto solo per SMB.
Client della condivisione file	Client NFS	Macchina virtuale Storage Gateway	Dati TCP o UDP NFSv3	111	✓	✓	✓*	Trasferimento di dati per la condivisione di file (solo per NFS v3) *Richiesto solo per NFS.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Client della condivisione file	Client NFS	Macchina virtuale Storage Gateway	NFS TCP o UDP	2049	✓	✓	✓*	Condivisione di file e trasferimento di dati *Richiesto solo per NFS v3 e v4.
Client della condivisione file	Client NFS	Macchina virtuale Storage Gateway	TCP o UDP NFSv3	20048	✓	✓	✓*	Condivisione di file e trasferimento dati *Richiesto solo per NFSv3
Client della condivisione file	Client NFS	Macchina virtuale Storage Gateway	TCP o UDP NFSv3	8750	✓	✓	✓*	Quota di condivisione dei file *Richiesto solo per NFSv3

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Client della condivisione file	Client SMB	Macchina virtuale Storage Gateway	TCP o UDP SMBv2	139	✓	✓	✓*	Servizio di sessione di trasferimento dati per la condivisione di file *Necessario solo per le PMI

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Simple Storage Service (Amazon S3)	Macchina virtuale Storage Gateway	Endpoint del servizio Amazon S3	TCP/ HTTPS	443	✓	✓	✓	Per la comunicazione dalla VM Storage Gateway all'endpoint del AWS servizio. Per informazioni sugli endpoint di servizio, vedere Consentire l'accesso AWS allo Storage Gateway tramite firewall e router.

L'illustrazione seguente mostra il flusso del traffico di rete per una distribuzione di base di S3 File Gateway.



Requisiti di rete e di firewall per l'appliance hardware Storage Gateway

Ogni appliance hardware Storage Gateway richiede i seguenti servizi di rete:

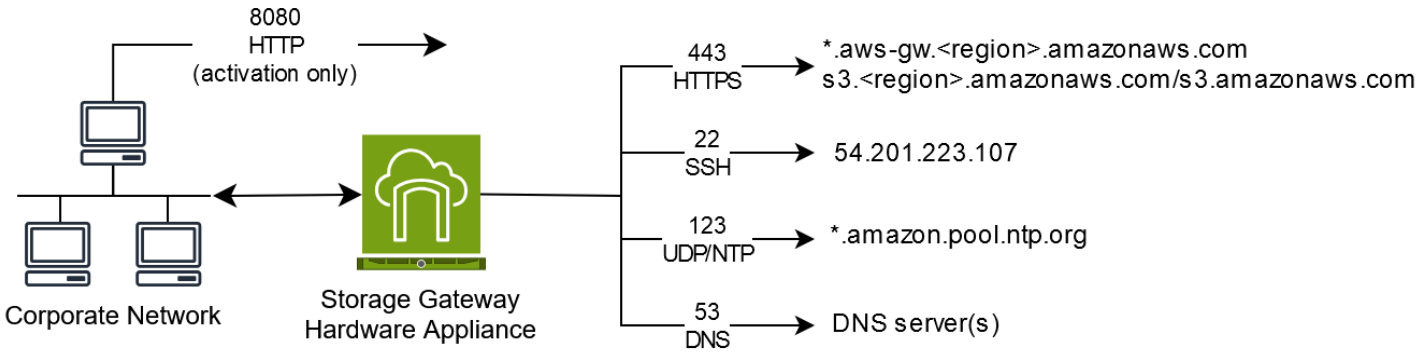
- Accesso a Internet: una connessione di rete a Internet sempre attiva tramite un'interfaccia di rete sul server.
- Servizi DNS: servizi DNS per la comunicazione tra l'appliance hardware e il server DNS.
- Tempo di sincronizzazione: un servizio orario Amazon NTP configurato automaticamente deve essere sempre raggiungibile.
- Indirizzo IP: un indirizzo DHCP o statico IPv4 assegnato. Non è possibile assegnare un IPv6 indirizzo.

Sul retro del server Dell PowerEdge R640 sono presenti cinque porte di rete fisiche. Da sinistra a destra (guardando la parte posteriore del server) queste porte sono le seguenti:

1. iDRAC
2. `em1`
3. `em2`

4. em3
5. em4

È possibile utilizzare la porta iDRAC per la gestione remota del server.



Un'appliance hardware richiede le seguenti porte per il funzionamento.

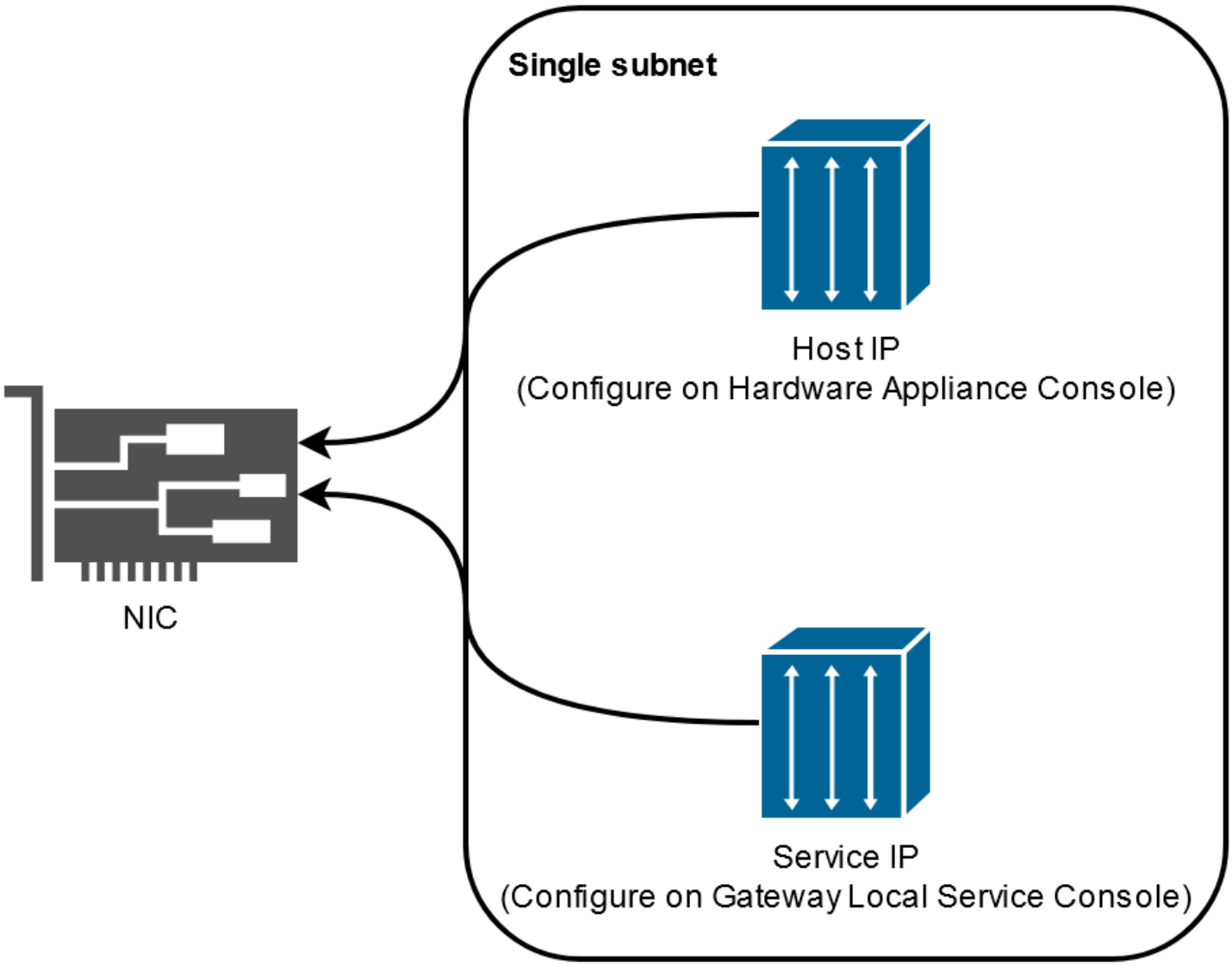
Protocollo	Porta	Direzione	Origine	Destinazione	Utilizzo
SSH	22	In uscita	Appliance hardware	`54.201.223.107`	Canale di supporto
DNS	53	In uscita	Appliance hardware	Server DNS	Risoluzione dei nomi
UDP/NTP	123	In uscita	Appliance hardware	`*.amazon.pool.ntp.org`	Sincronizzazione oraria
HTTPS	443	In uscita	Appliance hardware	`*.amazonaws.com`	Trasferimento dei dati
HTTP	8080	In entrata	AWS	Appliance hardware	Attivazione (solo brevemente)

Per funzionare in modo corretto, un'appliance hardware richiede le seguenti impostazioni di rete e firewall:

- Configurare tutte le interfacce di rete connesse nella console hardware.
- Assicurarsi che ogni interfaccia di rete si trovi in una sottorete univoca.
- Fornire a tutte le interfacce di rete connesse l'accesso in uscita agli endpoint elencati nel diagramma precedente.
- Configurare almeno un'interfaccia di rete per supportare l'appliance hardware. Per ulteriori informazioni, consulta Configurazione dei parametri di rete dell'apparecchiatura hardware.

> **Note**
>
> Per un'illustrazione che mostra la parte posteriore del server con le relative porte, vedere. Installazione fisica del dispositivo hardware

Tutti gli indirizzi IP sulla stessa interfaccia di rete (NIC), sia per un gateway che per un host, devono trovarsi nella stessa sottorete. La figura seguente illustra lo schema di assegnazione di indirizzi.



Per ulteriori informazioni sull'attivazione e la configurazione di un dispositivo hardware, vedere. Utilizzo dell'appliance hardware AWS Storage Gateway

Consentire Gateway di archiviazione AWS l'accesso tramite firewall e router

Il gateway richiede l'accesso ai seguenti endpoint del servizio Storage Gateway con AWS cui comunicare. Durante la configurazione del gateway, seleziona il tipo di endpoint per il gateway in base all'ambiente di rete. Se si utilizza un firewall o un router per filtrare o limitare il traffico di rete, è necessario configurare il firewall e/o il router affinché consentano questi endpoint di servizio per le comunicazioni in uscita ad AWS.

> **Note**
>
> Se si configurano endpoint VPC privati per lo Storage Gateway da utilizzare per la connessione e il trasferimento di dati da e verso AWS, il gateway non richiede l'accesso alla rete Internet pubblica. Per ulteriori informazioni, consulta Attivazione di un gateway in un cloud privato virtuale.

> **Important**
>
> Sostituisci *region* i seguenti esempi di endpoint con la Regione AWS stringa corretta per il tuo gateway, ad esempio. `us-west-2`
> Sostituiscilo *amzn-s3-demo-bucket* con il nome effettivo del bucket Amazon S3 nella tua distribuzione. Puoi anche utilizzare un asterisco (*) al posto di *amzn-s3-demo-bucket* per creare una voce jolly nelle regole del firewall, che consentirà di elencare gli endpoint del servizio per tutti i nomi dei bucket.
> Se i gateway sono distribuiti negli Stati Uniti d'America o Regioni AWS in Canada e richiedono connessioni endpoint conformi allo standard FIPS (Federal Information Processing Standard), sostituiscili con. *s3* `s3-fips`

Tipi di endpoint

Endpoint standard

Questi endpoint supportano il IPv4 traffico tra l'appliance gateway e. AWS

Il seguente endpoint di servizio è richiesto da tutti i gateway per le operazioni head-bucket.

```
bucket-name.s3.region.amazonaws.com:443
```

I seguenti endpoint di servizio sono richiesti da tutti i gateway per le operazioni control path (`anon-cp`,`client-cp`,`proxy-app`) e data path (). `dp-1`

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
```

Il seguente endpoint di servizio gateway è obbligatorio per effettuare chiamate API.

```
storagegateway.region.amazonaws.com:443
```

L'esempio seguente è un endpoint di servizio gateway nella regione Stati Uniti occidentali (Oregon) (`us-west-2`).

```
storagegateway.us-west-2.amazonaws.com:443
```

Endpoint dual-stack

Questi endpoint supportano IPv4 e gestiscono il IPv6 traffico tra il dispositivo gateway e. AWS

Il seguente endpoint di servizio dual-stack è richiesto da tutti i gateway per le operazioni head-bucket.

```
bucket-name.s3.dualstack.region.amazonaws.com:443
```

I seguenti endpoint di servizio dual-stack sono richiesti da tutti i gateway per le operazioni relative al percorso di controllo (attivazione, controlplane, proxy) e al percorso dei dati (dataplane).

```
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
```

Il seguente endpoint di servizio gateway dual-stack è necessario per effettuare chiamate API.

```
storagegateway.region.api.aws:443
```

L'esempio seguente è un endpoint di servizio gateway dual-stack nella regione Stati Uniti occidentali (Oregon) (). `us-west-2`

```
storagegateway.us-west-2.api.aws:443
```

Endpoint del servizio Amazon S3

Amazon S3 File Gateway richiede i seguenti tre tipi di endpoint per connettersi al servizio Amazon S3:

Endpoint del servizio Amazon S3

> **Note**
>
> Solo per questo endpoint, non sostituirlo `s3` con `s3-fips` implementazioni conformi a FIPS.

```
s3.amazonaws.com
```

Endpoint regionali Amazon S3

```
s3.region.amazonaws.com (Standard)
s3.dualstack.region.amazonaws.com (Dual-stack)
```

L'esempio seguente mostra un endpoint regionale Amazon S3 nella regione Stati Uniti orientali (Ohio) (). `us-east-2`

```
s3.us-east-2.amazonaws.com
s3.dualstack.us-east-2.amazonaws.com
```

L'esempio seguente mostra gli endpoint regionali Amazon S3 standard e dual-stack conformi a FIPS nella regione Stati Uniti occidentali (California settentrionale) (). `us-west-1`

```
s3-fips.us-west-1.amazonaws.com
s3-fips.dualstack.us-west-1.amazonaws.com
```

Gli esempi seguenti mostrano gli endpoint regionali Amazon S3 standard e dual-stack utilizzati dalle regioni: AWS GovCloud (US)

```
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))
s3-fips.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))
s3-fips.dualstack.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS
 dual-stack))
s3-fips.dualstack.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS
 dual-stack))
s3.dualstack.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Dual-stack))
```

```
s3.dualstack.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Dual-stack))
```

> **Note**
>
> Se il gateway non è in grado di determinare Regione AWS dove si trova il bucket Amazon S3, questo endpoint di servizio viene impostato come impostazione predefinita. `s3.us-east-1.amazonaws.com` Ti consigliamo di consentire l'accesso alla regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`) oltre a quella in Regioni AWS cui è attivato il gateway e dove si trova il tuo bucket Amazon S3.

Endpoint bucket Amazon S3

```
bucket-name.s3.region.amazonaws.com (Standard)
bucket-name.s3.dualstack.region.amazonaws.com (Dual-stack)
```

Gli esempi seguenti mostrano gli endpoint dei bucket Amazon S3 standard e dual-stack per un bucket denominato *amzn-s3-demo-bucket* nella regione Stati Uniti orientali (Ohio) (). `us-east-2`

```
amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com (Standard)
amzn-s3-demo-bucket.s3.dualstack.us-east-2.amazonaws.com (Dual-stack)
```

Gli esempi seguenti mostrano gli endpoint bucket Amazon S3 standard e dual-stack conformi a FIPS per un bucket denominato nella regione (Stati Uniti orientali) (). *amzn-s3-demo-bucket1* AWS GovCloud `us-gov-east-1`

```
amzn-s3-demo-bucket1.s3-fips.us-gov-east-1.amazonaws.com (FIPS)
amzn-s3-demo-bucket1.s3-fips.dualstack.us-gov-east-1.amazonaws.com (FIPS dual-stack)
```

Oltre agli endpoint del servizio Storage Gateway e Amazon S3, Storage Gateway richiede VMs anche l'accesso di rete ai seguenti server NTP:

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
```

```
3.amazon.pool.ntp.org
```

Per ulteriori informazioni sugli endpoint supportati Regioni AWS e di servizio, vedere Storage Gateway nel Riferimenti generali di AWS.

Configurazione dei gruppi di sicurezza per la tua istanza Amazon EC2 gateway

Nel Gateway di archiviazione AWS, un gruppo di sicurezza controlla il traffico verso la tua istanza Amazon EC2 gateway. Quando configuri un gruppo di sicurezza, tieni presente quanto segue:

- Il gruppo di sicurezza non deve permettere connessioni in entrata dall'esterno di Internet. Deve consentire solo alle istanze al suo interno di comunicare con il gateway.

  Se devi consentire alle istanze di connettersi al gateway dall'esterno del relativo gruppo di sicurezza, ti consigliamo di consentire le connessioni solo sulla porta 80 (per l'attivazione).
- Se desideri attivare il gateway da un EC2 host Amazon esterno al gruppo di sicurezza del gateway, consenti le connessioni in entrata sulla porta 80 dall'indirizzo IP di quell'host. Se non puoi determinare l'indirizzo IP dell'host di attivazione, apri la porta 80, attiva il gateway e, ad attivazione eseguita, chiudi l'accesso alla porta.
- Consenti l'accesso alla porta 22 solo se la utilizzi Supporto per la risoluzione dei problemi. Per ulteriori informazioni, consulta Vuoi aiutarci Supporto a risolvere i problemi del tuo gateway Amazon EC2 .

Per informazioni sulle porte da aprire per il gateway, consulta Requisiti delle porte.

Hypervisor supportati e requisiti di hosting

È possibile eseguire Storage Gateway in locale come appliance di macchina virtuale (VM) o dispositivo hardware fisico oppure come AWS istanza Amazon. EC2

Storage Gateway supporta le seguenti versioni di hypervisor e host:

- VMware ESXi Hypervisor (versione 7.0 o 8.0): per questa configurazione, è necessario anche un client VMware vSphere per connettersi all'host.
- Microsoft Hyper-V Hypervisor (2019, 2022 o 2025): per questa configurazione, è necessario un Microsoft Hyper-V Manager su un computer client Microsoft Windows per connettersi all'host.

- Macchina virtuale basata su kernel (KVM) Linux: una tecnologia di virtualizzazione gratuita e open-source. KVM è incluso in tutte le versioni di Linux 2.6.20 e successive. Storage Gateway è testato e supportato per le distribuzioni CentOS/RHEL 7.7, RHEL 8.6 Ubuntu 16.04 LTS e Ubuntu 18.04 LTS. Qualsiasi altra distribuzione Linux moderna può funzionare, ma la funzione o le prestazioni non sono garantite. Si consiglia questa opzione se si dispone già di un ambiente KVM attivo e si ha già familiarità con il funzionamento di KVM.
- Nutanix AHV (Acropolis Hypervisor) a partire dalla versione 10.0.1.1: una piattaforma di virtualizzazione basata su KVM integrata nella soluzione di infrastruttura iperconvergente (HCI) Nutanix.
- EC2 Istanza Amazon: Storage Gateway fornisce un'Amazon Machine Image (AMI) che contiene l'immagine della macchina virtuale del gateway. Per informazioni su come implementare un gateway su Amazon EC2, consultaImplementa un EC2 host Amazon predefinito per S3 File Gateway.
- Storage Gateway Hardware Appliance: Storage Gateway fornisce un'appliance hardware fisica come opzione di implementazione locale per sedi con un'infrastruttura di macchine virtuali limitata.

> **Note**
>
> Storage Gateway non supporta il ripristino di un gateway da una macchina virtuale creata da un'istantanea o da un clone di un'altra macchina virtuale gateway o dall'Amazon AMI. EC2
> Se la macchina virtuale gateway non funziona correttamente, attivare un nuovo gateway e ripristinare i dati su quel gateway. Per ulteriori informazioni, consulta Ripristino da un arresto imprevisto della macchina virtuale.
> Storage Gateway non supporta il ballooning di memoria dinamica e memoria virtuale.

Client NFS e SMB supportati per File Gateway

File Gateway supporta i seguenti client:

Versione del sistema operativo	Versione del kernel	Protocolli supportati
Amazon Linux 2023	6.1 LTS	NFSv46,1, NFSv3
Amazon Linux 2	5,10 LITRI	NFSv45,1, NFSv3

Versione del sistema operativo	Versione del kernel	Protocolli supportati
RHEL 9	5,14	NFSv45,1, NFSv3
REGOLA 8.10	4,18	NFSv44,1, NFSv3
USO 15	6.4	NFSv4.1, NFSv3
Ubuntu 24.04 LTS	6.8 LITRI	NFSv46,1, NFSv3
Ubuntu 22.04 LTS	5,15 LITRI	NFSv45,1, NFSv3
Microsoft Windows Server 2025		SMBv2, SMBv3, NFSv3
Microsoft Windows Server 2022		SMBv2, SMBv3, NFSv3
Microsoft Windows 11		SMBv2, SMBv3, NFSv3
Microsoft Windows 10		SMBv2, SMBv3, NFSv3

> **Note**
>
> La crittografia Server Message Block (SMB) richiede client che supportano i dialetti SMB v3.

Operazioni di file system supportate per File Gateway

Il client NFS o SMB può scrivere, leggere, eliminare, rinominare e troncare i file. Quando i client inviano delle scritture a Gateway di archiviazione AWS, queste scrivono nella cache locale in modo sincrono. Quindi, scrive su Amazon S3 in modo asincrono tramite trasferimenti ottimizzati. Le letture vengono servite automaticamente tramite la cache locale. Se i dati non sono disponibili, vengono recuperati tramite S3 come cache read-through.

Le operazioni di lettura e scrittura sono ottimizzate in modo tale che solo le parti modificate o richieste vengano tramite gateway. Elimina gli oggetti rimossi da Amazon S3. Le directory vengono gestite come oggetti cartella in S3, utilizzando la stessa sintassi della console Amazon S3.

Le operazioni HTTP quali `GET`, `PUT`, `UPDATE` e `DELETE` possono modificare i file in una condivisione file. Queste operazioni sono conformi alle funzioni atomiche di creazione, lettura, aggiornamento ed eliminazione (CRUD).

Gestione dei dischi locali per il gateway

La macchina virtuale (VM) gateway utilizza i dischi locali allocati in locale per il buffering e l'archiviazione. Un File Gateway creato su un' EC2 istanza Amazon utilizzerà i volumi Amazon EBS come dischi locali. Il numero e la dimensione dei dischi da allocare per il gateway dipende da te. Il gateway utilizza lo storage cache da te allocato per fornire un accesso a bassa latenza ai dati a cui hai avuto accesso di recente. I File Gateway richiedono almeno un disco da 150 GiB da utilizzare come cache. Dopo la configurazione e l'implementazione iniziali del gateway, è possibile aggiungere altri dischi per l'archiviazione della cache man mano che le richieste di carico di lavoro aumentano. Questa sezione contiene i seguenti argomenti, che descrivono concetti e procedure relativi alla gestione dei dischi locali.

Argomenti

- Determinazione della quantità di archiviazione su disco locale- Scopri come determinare il numero e la dimensione dei dischi di cache locale da allocare per File Gateway.
- Configurazione di una memoria cache aggiuntiva- Scopri come aumentare la capacità di archiviazione della cache di File Gateway man mano che le esigenze dell'applicazione cambiano.
- Utilizzo dello storage temporaneo con i gateway EC2 - Scopri come prevenire la perdita di dati quando utilizzi lo storage temporaneo su disco con File Gateway.

Determinazione della quantità di archiviazione su disco locale

Quando implementate un S3 File Gateway , considerate la quantità di disco di cache da allocare. S3 File Gateway utilizza un algoritmo utilizzato meno di recente per eliminare automaticamente i dati dalla cache. La cache su un S3 File Gateway è condivisa tra tutte le condivisioni di file su quel gateway. Se disponi di più condivisioni attive, è importante notare che un utilizzo intensivo di una condivisione potrebbe influire sulla quantità di risorse di cache a cui un'altra condivisione ha accesso, con possibili ripercussioni sulle prestazioni.

Quando si determina la quantità di disco di cache necessaria per un determinato carico di lavoro, è importante notare che è sempre possibile aggiungere un disco cache al gateway (fino alle quote

correnti su S3 File Gateway), ma non è possibile ridurre la cache per un determinato gateway. È possibile eseguire un'analisi di base sul set di dati per determinare la giusta quantità di disco di cache, ma non esiste un modo per determinare esattamente quanti dati siano «caldi» e debbano essere archiviati localmente, anziché «freddi» e possano essere trasferiti su più livelli nel cloud. I carichi di lavoro cambiano nel tempo e S3 File Gateway offre flessibilità ed elasticità legate alla quantità di risorse che possono essere consumate. La quantità di cache può sempre essere aumentata, quindi l'approccio più conveniente è spesso partire da un valore ridotto e aumentarlo in base alle esigenze.

È possibile utilizzare un'approssimazione iniziale di 150 GiB per effettuare il provisioning dei dischi per l'archiviazione della cache durante la configurazione del gateway. Puoi quindi utilizzare i parametri CloudWatch operativi di Amazon per monitorare l'utilizzo dello storage della cache e fornire più spazio di archiviazione in base alle esigenze utilizzando la console. Per informazioni sull'uso dei parametri e sull'impostazione di allarmi, consulta Prestazioni e ottimizzazione.

> **Note**
>
> Le risorse di storage fisico sottostanti sono rappresentate come un archivio dati in VMware. Quando si distribuisce la macchina virtuale del gateway, si sceglie un datastore in cui archiviare i file VM. Quando si esegue il provisioning di un disco locale (ad esempio, da utilizzare come archiviazione cache), è possibile archiviare il disco virtuale nello stesso archivio dati della macchina virtuale o in un archivio dati diverso.
> Se disponi di più di un data store, ti consigliamo vivamente di sceglierne uno per l'archiviazione nella cache. Un data store supportato da un solo disco fisico sottostante può portare a prestazioni scadenti in alcune situazioni quando viene utilizzato per il backup di entrambi gli archivi della cache. Questo vale anche se il backup è una configurazione RAID meno performante come. RAID1

Configurazione di una memoria cache aggiuntiva

Man mano che le esigenze dell'applicazione cambiano, è possibile aumentare la capacità di archiviazione della cache del gateway. È possibile aggiungere capacità di archiviazione al gateway senza interrompere la funzionalità o causare tempi di inattività. Quando aggiungi ulteriore spazio di archiviazione, esegui l'operazione con la macchina virtuale del gateway attivata.

> **Important**
>
> Quando aggiungi cache a un gateway esistente, devi creare nuovi dischi sull'hypervisor host del gateway o sull'istanza Amazon. EC2 Non rimuovere o modificare le dimensioni dei dischi esistenti che sono già stati allocati come cache.

Per configurare una memoria cache aggiuntiva per il gateway

1. Effettua il provisioning di uno o più nuovi dischi sull'host del gateway, sull'hypervisor o sull'istanza Amazon. EC2 Per informazioni su come effettuare il provisioning di un disco in un hypervisor, consulta la documentazione dell'hypervisor. Per informazioni sul provisioning di volumi Amazon EBS per EC2 un'istanza Amazon, consulta i volumi Amazon EBS nella Amazon Elastic Compute Cloud User Guide for Linux Instances. Nei passaggi seguenti, configurerai questo disco come storage cache.
2. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
3. Nel riquadro di navigazione, scegliere Gateways.
4. Nell'elenco, cerca e seleziona il tuo gateway.
5. Dal menu Azioni, scegli Configura l'archiviazione della cache.
6. Nella sezione Configura l'archiviazione della cache, identifica i dischi di cui hai effettuato il provisioning. Se i dischi non sono visualizzati, scegli l'icona di aggiornamento per aggiornare l'elenco. Per ogni disco, scegli Cache dal menu a discesa Allocato a.

   > **Note**
   >
   > La cache è l'unica opzione disponibile per l'allocazione dei dischi su un File Gateway.

7. Per salvare le impostazioni di configurazione, seleziona Salva.

Utilizzo dello storage temporaneo con i gateway EC2

Questa sezione descrive le operazioni necessarie per evitare la perdita di dati quando si seleziona un disco temporaneo come storage della cache del gateway.

I dischi temporanei forniscono uno storage temporaneo a livello di blocco per la tua istanza Amazon. EC2 I dischi temporanei sono ideali per l'archiviazione temporanea di dati che cambiano frequentemente, come i dati nella memoria cache di un gateway. Quando avvii il gateway con

un'Amazon EC2 Amazon Machine Image e il tipo di istanza selezionato supporta lo storage temporaneo, i dischi temporanei vengono elencati automaticamente. Puoi selezionare uno dei dischi per archiviare i dati della cache del gateway. Per ulteriori informazioni, consulta Amazon EC2 Instance Store nella Amazon EC2 User Guide.

È possibile prevenire tale perdita di dati seguendo i passaggi prima di riavviare o arrestare l' EC2 istanza che ospita il gateway.

> **Important**
>
> Se interrompi e avvii un EC2 gateway Amazon che utilizza lo storage temporaneo, il gateway sarà permanentemente offline. Questo accade perché il disco di storage fisico viene sostituito. Non esiste alcuna soluzione alternativa per questo problema. L'unica soluzione è eliminare il gateway e attivarne uno nuovo su una nuova istanza. EC2

Questi passaggi della procedura seguente sono specifici per File Gateway.

Per prevenire la perdita di dati nei File Gateway che utilizzano dischi temporanei

1. Interrompi tutti i processi di scrittura su Amazon S3.
2. Iscriviti per ricevere notifiche da CloudWatch Events. Per informazioni, consulta Ricevere notifiche sulle operazioni sui file.
3. Chiama l'NotifyWhenUploaded API per ricevere una notifica quando i dati scritti, fino alla perdita dello storage temporaneo, sono stati archiviati in modo duraturo in Amazon S3.
4. Attendi che l'API si completi e riceverai un id notifica.

   Ricevi un CloudWatch evento con lo stesso ID di notifica.
5. Verificare che il parametro `CachePercentDirty` per la condivisione file sia 0. Ciò conferma che tutti i tuoi dati sono stati scritti su Amazon S3. Per informazioni sui parametri delle condivisioni di file, consulta Comprensione delle metriche relative alla condivisione dei file.
6. Ora puoi riavviare o arrestare File Gateway senza rischiare di perdere alcun dato.

Utilizzo dell'appliance hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

L'appliance hardware AWS Storage Gateway è un'appliance hardware fisica con il software Storage Gateway preinstallato su una configurazione server convalidata. È possibile gestire le appliance hardware della distribuzione dalla pagina di panoramica dell'appliance hardware nella console. Gateway di archiviazione AWS

L'appliance hardware è un server 1U ad alte prestazioni che è possibile distribuire nel proprio data center, oppure on-premise all'interno di un firewall aziendale. Quando acquisti e attivi l'appliance hardware, il processo di attivazione associa l'appliance hardware al tuo. Account AWS Dopo l'attivazione, l'appliance hardware viene visualizzata nella console nella pagina di panoramica dell'appliance hardware. È possibile configurare l'appliance hardware come tipo S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway. La procedura utilizzata per distribuire questi tipi di gateway su un'appliance hardware è la stessa utilizzata su una piattaforma virtuale.

Per un elenco delle aree supportate Regioni AWS in cui l'appliance hardware AWS Storage Gateway è disponibile per l'attivazione e l'uso, vedere AWS Storage Gateway Hardware Appliance Regions nel. Riferimenti generali di AWS

Nelle sezioni seguenti sono disponibili istruzioni su come configurare, montare su rack, alimentare, configurare, attivare, avviare, utilizzare ed eliminare un'appliance hardware AWS Storage Gateway.

Argomenti

- Configurazione dell'appliance hardware AWS Storage Gateway
- Installazione fisica del dispositivo hardware
- Accesso alla console dell'apparecchiatura hardware

- Configurazione dei parametri di rete dell'apparecchiatura hardware
- Attivazione del dispositivo hardware AWS Storage Gateway
- Creazione di un gateway sul tuo dispositivo hardware
- Configurazione di un indirizzo IP del gateway sull'appliance hardware
- Rimozione del software gateway dal dispositivo hardware
- Eliminazione del dispositivo hardware AWS Storage Gateway

Configurazione dell'appliance hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Dopo aver ricevuto l'appliance hardware Storage Gateway, si utilizza la console locale dell'appliance hardware per configurare la rete in modo da fornire una connessione sempre attiva e attivare l'appliance. AWS L'attivazione associa l'appliance all' AWS account utilizzato durante il processo di attivazione. Dopo l'attivazione dell'appliance, è possibile avviare S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway dalla console Storage Gateway.

Installare e configurare l'appliance hardware

1. Montare l'appliance su rack e collegare l'alimentazione e le connessioni di rete. Per ulteriori informazioni, consulta Installazione fisica del dispositivo hardware.
2. Imposta gli indirizzi Internet Protocol versione 4 (IPv4) per l'appliance hardware (l'host). Per ulteriori informazioni, consulta Configurazione dei parametri di rete dell'apparecchiatura hardware.
3. Attiva l'appliance hardware nella pagina di panoramica dell'appliance hardware della console nella AWS regione di tua scelta. Per ulteriori informazioni, consulta Attivazione del dispositivo hardware AWS Storage Gateway.

4. Crea un gateway sul tuo dispositivo hardware. Per ulteriori informazioni, consulta Crea il tuo gateway.

   Puoi configurare i gateway sul tuo dispositivo hardware nello stesso modo in cui configuri i gateway su VMware ESXi Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) o Amazon. EC2

Aumento dello storage della cache utilizzabile

È possibile aumentare lo spazio di archiviazione utilizzabile sull'appliance hardware da 5 TB a 12 TB. In questo modo si ottiene una cache più ampia per l'accesso a bassa latenza ai dati in ingresso. AWS Se hai ordinato il modello da 5 TB, puoi aumentare lo spazio di archiviazione utilizzabile a 12 TB acquistando cinque unità a stato solido da 1,92 SSDs TB.

È quindi possibile aggiungerli all'appliance hardware prima di attivarla. Se l'appliance hardware è già stata attivata e di desidera aumentare l'archiviazione utilizzabile sull'appliance a 12 TB, procedere nel seguente modo:

1. Ripristina le impostazioni di fabbrica dell'appliance hardware. Contatta l' AWS assistenza per istruzioni su come eseguire questa operazione.
2. Aggiungi cinque 1,92 TB SSDs all'appliance.

Opzioni della scheda di interfaccia di rete

A seconda del modello di dispositivo ordinato, può essere fornito con una scheda di rete 10G-Base-T in RJ45 rame o una scheda di rete DA/SFP+ 10G.

- Configurazione 10 NIC: G-Base-T
  - Utilizzare CAT6 cavi per 10G o CAT5 (e) per 1G
- Configurazione NIC 10G DA/SFP+:
  - Utilizzare cavi Twinax in rame Direct Attach fino a 5 metri
  - Moduli ottici SFP+ compatibili con Dell/Intel (SR o LR)
  - Ricetrasmettitore in rame SFP/SFP+ per 1 o 10G-Base-T G-Base-T

Installazione fisica del dispositivo hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

L'appliance ha un fattore di forma 1U e si inserisce in un rack da 19 pollici standard conforme alla Commissione elettrotecnica internazionale (IEC).

Prerequisiti

Per installare l'appliance hardware, sono necessari i seguenti componenti:

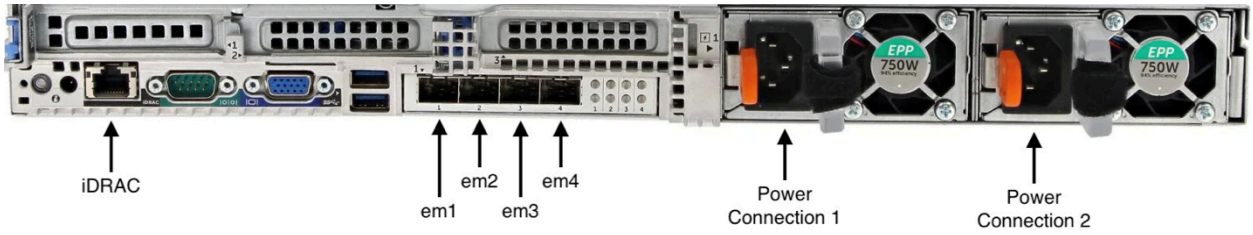
- Cavi di alimentazione: uno necessario, due consigliati.
- Cablaggio di rete supportato (a seconda della scheda di interfaccia di rete (NIC) incluso nell'appliance hardware). DAC Twinax in rame, modulo ottico SFP+ (compatibile con Intel) o ricetrasmettitore in rame da SFP a Base-T.
- Tastiera e monitor, oppure una soluzione tastiera, video e mouse (KVM).

> **Note**
>
> Prima di effettuare la procedura seguente, verificare di soddisfare tutti i requisiti per l'appliance hardware Storage Gateway come descritto in Requisiti di rete e di firewall per l'appliance hardware Storage Gateway.

Per installare fisicamente il dispositivo hardware

1. Estrai dalla confezione il dispositivo hardware e segui le istruzioni contenute nella confezione per montare il server su rack.

L'immagine seguente mostra la parte posteriore del dispositivo hardware con porte per il collegamento di alimentazione, ethernet, monitor, tastiera USB e iDRAC.
dispositivo hardware (uno posteriore) con etichette per connettori di rete e di alimentazione.

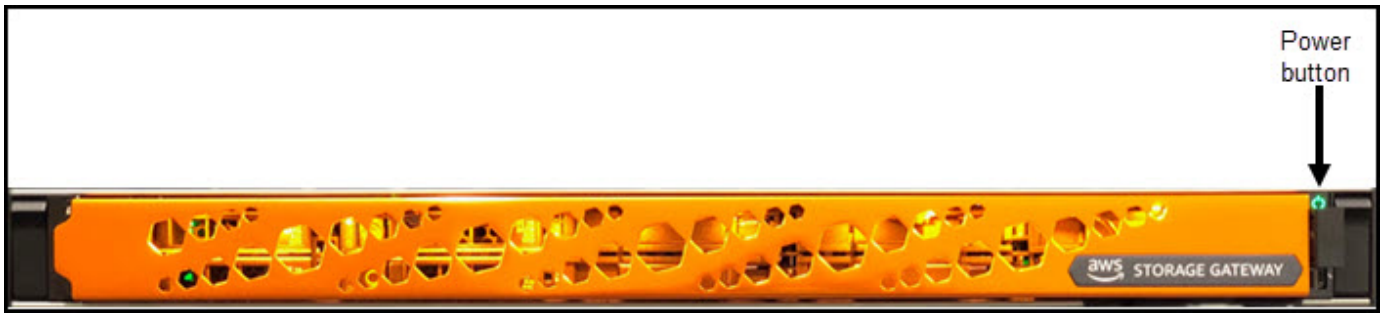


dispositivo hardware sul retro con etichette per connettori di rete e di alimentazione.

2. Collegare all'alimentazione ciascuno dei due alimentatori. È possibile collegarlo a una sola connessione di alimentazione, ma consigliamo di collegare entrambi gli alimentatori per garantire la ridondanza.
3. Inserire il cavo Ethernet nella porta `em1` per una connessione Internet sempre attiva. La porta `em1` è la prima delle quattro porte di rete fisiche nella parte posteriore, da sinistra a destra.

> **Note**
>
> L'appliance hardware non supporta il trunking VLAN. Configurare la porta a cui si sta collegando l'appliance hardware come porta senza trunking VLAN.

4. Collegare la tastiera e il monitor.
5. Accendere il server premendo il pulsante Power sul pannello anteriore, come mostrato nell'immagine seguente.
parte anteriore dell'appliance hardware con etichetta del pulsante di accensione.



parte anteriore dell'appliance hardware con etichetta del pulsante di accensione.

Approfondimenti

[Accesso alla console dell'apparecchiatura hardware]

Accesso alla console dell'apparecchiatura hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Quando si accende l'appliance hardware, la console dell'appliance hardware viene visualizzata sul monitor. La console dell'appliance hardware presenta un'interfaccia utente specifica AWS che è possibile utilizzare per impostare una password di amministratore, configurare i parametri di rete iniziali e aprire un canale di supporto per. AWS

Per utilizzare la console dell'appliance hardware, immettete il testo dalla tastiera e utilizzate i `Left Arrow` tasti Up `DownRight`,, e per spostarvi sullo schermo nella direzione indicata. Utilizzare il tasto `Tab` per andare avanti in ordine tra gli elementi sullo schermo. In alcune configurazioni, è possibile utilizzare la combinazione di tasti `Shift+Tab` per spostarsi sequenzialmente all'indietro. Utilizzare il tasto `Enter` per salvare le selezioni oppure per scegliere un pulsante sullo schermo.

La prima volta che viene visualizzata la console dell'appliance hardware, viene visualizzata la pagina di benvenuto e all'utente viene richiesto di impostare una password per l'account utente amministratore prima di poter accedere alla console.

Per impostare una password di amministratore

- Alla richiesta di impostazione della password di accesso, procedi come segue:

  a. In Set Password (Imposta password), immettere una password e premere `Down arrow`.
  b. In Confirm (Conferma), immettere nuovamente la password e quindi scegliere Save Password (Salva password).

Dopo aver impostato la password, viene visualizzata la home page della console hardware. La home page mostra le informazioni di rete per le interfacce di rete em1, em2, em3 ed em4 e presenta le seguenti opzioni di menu:

- Configura rete
- Apri Service Console
- Modifica della password
- Disconnettersi
- Apri Support Console

Approfondimenti

Configurazione dei parametri di rete dell'apparecchiatura hardware

Configurazione dei parametri di rete dell'apparecchiatura hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Dopo l'avvio dell'appliance hardware e aver impostato la password dell'utente amministratore nella console hardware come descritto inAccesso alla console dell'apparecchiatura hardware, utilizzare la procedura seguente per configurare i parametri di rete a cui l'appliance hardware possa connettersi. AWS

Per impostare un indirizzo di rete

1. Dalla home page, scegli Configura rete, quindi premi. `Enter` Viene visualizzata la pagina Configura rete. La pagina Configura rete mostra le informazioni IP e DNS per ciascuna delle 4 interfacce di rete dell'appliance hardware e include le opzioni di menu per configurare gli indirizzi DHCP o statici per ciascuna.
2. Per l'interfaccia em1, effettuate una delle seguenti operazioni:

   - Scegliete DHCP e premete `Enter` per utilizzare l' IPv4 indirizzo assegnato dal server DHCP (Dynamic Host Configuration Protocol) alla porta di rete fisica.

Annota questo indirizzo per utilizzarlo successivamente nella fase di attivazione.

- Scegli Statico e premi `Enter` per configurare un IPv4 indirizzo statico.

  Inserisci un indirizzo IP, una subnet mask, un gateway e un indirizzo del server DNS validi per l'interfaccia di rete em1.

  Al termine, scegli Salva, quindi premi `Enter` per salvare la configurazione.

> **Note**
>
> È possibile utilizzare questa procedura per configurare altre interfacce di rete oltre a em1. Se configuri altre interfacce, queste devono fornire la stessa connessione sempre attiva agli endpoint elencati nei requisiti. AWS
> Il Network Bonding e il Link Aggregation Control Protocol (LACP) non sono supportati dall'appliance hardware o da Storage Gateway.
> Si sconsiglia di configurare più interfacce di rete sulla stessa sottorete, in quanto ciò può talvolta causare problemi di routing.

Per disconnettersi dalla console hardware

1. Scegli Indietro e premi **`Enter`** per tornare alla home page.
2. Scegli Logout e premi `Enter` per tornare alla pagina di benvenuto.

Approfondimenti

Attivazione del dispositivo hardware AWS Storage Gateway

Attivazione del dispositivo hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione

AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Dopo aver configurato l'indirizzo IP, inserite questo indirizzo IP nella pagina Hardware della Gateway di archiviazione AWS console per attivare il dispositivo hardware. Il processo di attivazione registra l'appliance nell'account dell'utente. AWS

È possibile scegliere di attivare il dispositivo hardware in uno dei sistemi supportati. Regioni AWS Per un elenco delle aree supportate Regioni AWS, vedere Storage Gateway Hardware Appliance Regions nel Riferimenti generali di AWS.

Per attivare l'appliance hardware AWS Storage Gateway

1. Apri la Console di gestione Gateway di archiviazione AWS e accedi con le credenziali dell'account che desideri utilizzare per attivare l'hardware.

   > **Note**
   >
   > I seguenti requisiti sono necessari solo per l'attivazione:
   >
   > - Il browser deve trovarsi nella stessa rete dell'appliance hardware.
   > - Il firewall deve consentire l'accesso HTTP all'appliance sulla porta 8080 per il traffico in entrata.

2. Dal menu di navigazione a sinistra della pagina, scegli Hardware.
3. Scegli Attiva dispositivo.
4. Per Indirizzo IP, inserisci l'indirizzo IP che hai configurato per il dispositivo hardware, quindi scegli Connetti.

   Per ulteriori informazioni sulla configurazione dell'indirizzo IP, consulta Configurazione dei parametri di rete.
5. Per Nome, inserisci un nome per il dispositivo. I nomi possono contenere fino a 255 caratteri e non possono includere uno slash.
6. Per Fuso orario del dispositivo hardware inserisci il fuso orario locale da cui verrà generata la maggior parte del carico di lavoro per il gateway, quindi scegli Avanti.

Il fuso orario determina quando l'hardware effettua gli aggiornamenti; con l'orario pianificato per impostazione predefinita sulle 2 di notte ora locale. Idealmente, se il fuso orario è impostato correttamente, per impostazione predefinita gli aggiornamenti avverranno al di fuori dell'orario di lavoro.

7. Consulta i parametri di attivazione nella sezione relativa ai dettagli dell'apparecchiatura hardware. Puoi scegliere Precedente per tornare indietro e apportare modifiche, se necessario. Altrimenti, scegli Attiva per completare l'attivazione.

Nella pagina Panoramica del dispositivo hardware verrà visualizzato un banner che indica che il dispositivo hardware è stato attivato correttamente.

A questo punto, l'appliance è associata all'account. Il passaggio successivo consiste nel configurare e avviare un S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway sulla nuova appliance.

Approfondimenti

Creazione di un gateway sul tuo dispositivo hardware

Creazione di un gateway sul tuo dispositivo hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l' Gateway di archiviazione AWS Hardware Appliance non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

È possibile creare un S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway su qualsiasi appliance hardware AWS Storage Gateway presente nell'implementazione.

Per creare un gateway sull'appliance hardware

1. Accedi Console di gestione AWS e apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.

2. Segui le procedure descritte in Creazione del gateway per configurare, connettere e configurare il tipo di Storage Gateway che desideri implementare.

Al termine della creazione del gateway nella console Storage Gateway, il software Storage Gateway inizia automaticamente l'installazione sull'appliance hardware. Se si utilizza il Dynamic Host Configuration Protocol (DHCP), possono essere necessari dai 5 ai 10 minuti prima che un gateway venga visualizzato come online nella console. Per assegnare un indirizzo IP statico al gateway installato, vedere Configurazione di un indirizzo IP per il gateway.

Per assegnare un indirizzo IP statico al gateway installato, è necessario configurare le interfacce di rete del gateway in modo che le applicazioni possano utilizzarlo.

Approfondimenti

Configurazione di un indirizzo IP del gateway sull'appliance hardware

Configurazione di un indirizzo IP del gateway sull'appliance hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l' Gateway di archiviazione AWS Hardware Appliance non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Prima di attivare l'appliance hardware, è stato assegnato un indirizzo IP alla relativa interfaccia di rete fisica. Dopo aver attivato l'appliance e avviato lo Storage Gateway su di essa, è necessario assegnare un altro indirizzo IP alla macchina virtuale Storage Gateway in esecuzione sull'appliance hardware. Per assegnare un indirizzo IP statico a un gateway installato sul dispositivo hardware, configura l'indirizzo IP dalla console locale del gateway per quel gateway. Le applicazioni (come il client NFS o SMB) si connettono a questo indirizzo IP. È possibile accedere alla console locale del gateway dalla console dell'appliance hardware utilizzando l'opzione Open Service Console.

Per configurare l'indirizzo IP sull'appliance per farla funzionare con le applicazioni.

1. Sulla console hardware, scegli Open Service Console, quindi premi `Enter` per aprire la pagina di accesso per la console locale del gateway.
2. La pagina di accesso alla console Gateway di archiviazione AWS locale richiede di effettuare il login per modificare la configurazione di rete e altre impostazioni.

   L'account predefinito è `admin` e la password predefinita è `password`.

   > **Note**
   >
   > Si consiglia di modificare la password predefinita inserendo il numero corrispondente per Console del gateway dal menu principale Attivazione dell'appliance AWS : configurazione, eseguendo poi il comando `passwd`. Per informazioni su come eseguire il comando, consulta Esecuzione di comandi Storage Gateway sulla console locale. È inoltre possibile impostare la password dalla console Storage Gateway. Per ulteriori informazioni, consulta Impostazione della password della console locale dalla console Storage Gateway .

3. La pagina Attivazione dell'AWS appliance - Configurazione include le seguenti opzioni di menu:

   - Configurazione del proxy HTTP/SOCKS
   - Configurazione di rete
   - Test della connettività di rete
   - Visualizza il controllo delle risorse di sistema
   - Gestione del tempo di sistema
   - Informazioni sulla licenza
   - Prompt dei comandi

   > **Note**
   >
   > Alcune opzioni sono disponibili solo per tipi di gateway o piattaforme host specifici.

   Immettete il numero corrispondente per accedere alla pagina di configurazione della rete.

4. Effettuate una delle seguenti operazioni per configurare l'indirizzo IP del gateway:

- Per utilizzare l'indirizzo IP assegnato dal server DHCP (Dynamic Host Configuration Protocol), immettete il numero corrispondente per Configura DHCP, quindi immettete informazioni di configurazione DHCP valide nella pagina seguente.
- Per assegnare un indirizzo IP statico, inserisci il numero corrispondente per Configura IP statico, quindi inserisci un indirizzo IP e informazioni DNS valide nella pagina seguente.

> **Note**
>
> L'indirizzo IP specificato qui deve trovarsi nella stessa sottorete dell'indirizzo IP utilizzato durante l'attivazione dell'appliance hardware.

Per uscire dalla console locale del gateway

- Premere la sequenza di tasti `Crtl+]` (parentesi di chiusura). Viene visualizzata la console hardware.

> **Note**
>
> La combinazione di tasti precedente è l'unico modo per uscire dalla console locale del gateway.

Dopo che l'appliance hardware è stata attivata e configurata, l'appliance viene visualizzata nella console. Ora è possibile continuare la procedura di installazione e configurazione del gateway nella console Storage Gateway. Per istruzioni, consultare Configura il tuo Amazon S3 File Gateway.

Rimozione del software gateway dal dispositivo hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l' Gateway di archiviazione AWS Hardware Appliance non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per

fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Se non è più necessario uno Storage Gateway specifico distribuito su un'appliance hardware, è possibile rimuovere il software del gateway dall'appliance hardware. Dopo aver rimosso il software del gateway, è possibile scegliere di installare un nuovo gateway al suo posto o eliminare l'appliance hardware stessa dalla console Storage Gateway. Per rimuovere un software del gateway dall'appliance hardware, utilizzare la procedura seguente.

Rimuovere un gateway da un'appliance hardware

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Hardware dal pannello di navigazione sul lato sinistro della pagina della console, quindi scegli il nome dell'appliance hardware per l'appliance da cui desideri rimuovere il software gateway.
3. Dal menu a discesa Azioni, scegli Rimuovi gateway.

   Viene visualizzata la finestra di dialogo di conferma.
4. Verifica di voler rimuovere il software del gateway dall'appliance hardware specificata, quindi digita la parola `remove` nella casella di conferma.
5. Scegliete Rimuovi per rimuovere definitivamente il software del gateway.

> **Note**
>
> Dopo aver rimosso il software del gateway, non puoi annullare l'azione. Per determinati tipi di gateway, è possibile che con l'eliminazione si perdano dei dati, soprattutto quelli memorizzati nella cache. Per ulteriori informazioni sull'eliminazione di un gateway, consulta Eliminazione del gateway e rimozione delle risorse associate.

La rimozione di un gateway non elimina l'appliance hardware dalla console. L'appliance hardware rimane disponibile per future implementazioni del gateway.

Eliminazione del dispositivo hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Se non è più necessario un dispositivo hardware AWS Storage Gateway già attivato, è possibile eliminare completamente l'appliance dal proprio account AWS .

> **Note**
>
> Per spostare l'appliance su un altro AWS account o Regione AWS, è necessario prima eliminarla utilizzando la procedura seguente, quindi aprire il canale di supporto del gateway e contattarla Supporto per eseguire un soft reset. Per ulteriori informazioni, consulta Attivazione dell' Supporto accesso per risolvere i problemi del gateway ospitato in locale del gateway ospitato in locale.

Per eliminare l'appliance hardware

1. Se è stato installato un gateway nell'appliance hardware, è necessario prima rimuovere il gateway per eliminare l'appliance. Per istruzioni su come rimuovere un gateway dall'appliance hardware, consulta Rimozione del software gateway dal dispositivo hardware.
2. Nella pagina Hardware della console Storage Gateway, scegliere l'appliance hardware che si desidera eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack). Viene visualizzata la finestra di dialogo di conferma.
4. Verifica di voler eliminare l'appliance hardware specificata, quindi digita la parola delete nella casella di conferma e scegli Elimina.

Quando si elimina l'appliance hardware, vengono eliminate anche tutte le risorse associate con il gateway installato sull'appliance, ma i dati sull'appliance hardware stessa non vengono eliminati.

Crea il tuo gateway

Le sezioni di panoramica di questa pagina forniscono un riepilogo di alto livello di come funziona il processo di creazione dello Storage Gateway. Per step-by-step le procedure per creare un tipo specifico di gateway utilizzando la console Storage Gateway, vedere i seguenti argomenti:

- Crea e attiva un Amazon S3 File Gateway
- Crea e attiva un Amazon FSx File Gateway
- Crea e attiva un Tape Gateway
- Crea e attiva un Volume Gateway

Panoramica: attivazione del gateway

L'attivazione del gateway prevede la configurazione del gateway, la connessione AWS, la revisione delle impostazioni e l'attivazione.

Configurazione di un gateway

Per configurare Storage Gateway, è necessario innanzitutto scegliere il tipo di gateway che si desidera creare e la piattaforma host su cui eseguire l'appliance virtuale gateway. È quindi necessario scaricare il modello di appliance virtuale gateway per la piattaforma prescelta e distribuirlo nell'ambiente on-premise. Puoi anche implementare lo Storage Gateway come appliance hardware fisica che ordini dal tuo rivenditore preferito o come EC2 istanza Amazon nel tuo AWS ambiente cloud. Quando si distribuisce l'appliance gateway, si alloca lo spazio fisico locale su disco sull'host di virtualizzazione.

Connect a AWS

Il passaggio successivo consiste nel connettere il gateway a AWS. A tale scopo, devi innanzitutto scegliere il tipo di endpoint di servizio che desideri utilizzare per le comunicazioni tra l'appliance virtuale gateway e AWS i servizi nel cloud. Questo endpoint può essere accessibile dalla rete Internet pubblica o solo dall'interno del tuo Amazon VPC, dove hai il pieno controllo sulla configurazione di sicurezza della rete. È quindi necessario specificare l'indirizzo IP del gateway o la relativa chiave di attivazione, che è possibile ottenere collegandosi alla console locale sull'appliance gateway.

Rivedi e attiva

A questo punto, avrai l'opportunità di rivedere il gateway e le opzioni di connessione che hai scelto e, se necessario, apportare modifiche. Una volta che tutto è configurato come desideri puoi attivare il gateway. Prima di poter iniziare a utilizzare il gateway attivato, è necessario configurare alcune impostazioni aggiuntive e creare le risorse di archiviazione.

Panoramica: configurazione del gateway

Dopo aver attivato Storage Gateway, è necessario eseguire una configurazione aggiuntiva. In questa fase, si alloca lo storage fisico fornito sulla piattaforma host del gateway per utilizzarlo come cache o buffer di caricamento dall'appliance gateway. Quindi configuri le impostazioni per monitorare lo stato del gateway utilizzando Amazon CloudWatch Logs and CloudWatch alarms e aggiungi tag per identificare il gateway, se lo desideri. Prima di poter iniziare a utilizzare il gateway attivato e configurato, è necessario creare le risorse di archiviazione.

Panoramica: risorse di archiviazione

Dopo aver attivato e configurato Storage Gateway, è necessario creare risorse di archiviazione cloud da utilizzare. A seconda del tipo di gateway creato, utilizzerai la console Storage Gateway per creare volumi, nastri o condivisioni di file Amazon S3 o FSx Amazon Amazon da associare. Ogni tipo di gateway utilizza le rispettive risorse per emulare il tipo correlato di infrastruttura di archiviazione di rete e trasferisce i dati che scrivi su di esso nel cloud AWS .

Crea e attiva un Amazon S3 File Gateway

In questa sezione, puoi trovare istruzioni su come creare, distribuire e attivare un File Gateway in Gateway di archiviazione AWS.

Argomenti

- Configurazione di un Amazon S3 File Gateway
- Connect il tuo Amazon S3 File Gateway a AWS
- Rivedi le impostazioni e attiva il tuo Amazon S3 File Gateway
- Configura il tuo Amazon S3 File Gateway

Configurazione di un Amazon S3 File Gateway

Per configurare un nuovo S3 File Gateway

1. Apri Console di gestione AWS at https://console.aws.amazon.com/storagegateway/home/ e scegli Regione AWS dove vuoi creare il gateway.
2. Scegli Create gateway (Crea gateway) per aprire la pagina Set up gateway (Configura gateway).
3. Nella sezione Impostazioni gateway, procedi nel seguente modo:

   a. Per Gateway name (Nome gateway), inserire un nome per il gateway. Dopo aver creato il gateway, puoi cercare questo nome per trovarlo nelle pagine di elenco della Gateway di archiviazione AWS console.

   b. Per il Fuso orario del gateway, scegli il fuso orario locale per la parte del mondo in cui desideri implementare il gateway.
4. Nella sezione Opzioni gateway, per il tipo di gateway, scegli Amazon S3 File Gateway.
5. Nella sezione Opzioni piattaforma, procedi nel modo seguente:

   a. Per la piattaforma Host, scegli la piattaforma su cui vuoi implementare il tuo gateway. Quindi segui le istruzioni specifiche della piattaforma visualizzate nella pagina della console Storage Gateway per configurare la piattaforma host. Scegliere tra le seguenti opzioni:

      - VMware ESXi— Scarica, distribuisci e configura la macchina virtuale gateway utilizzando. VMware ESXi
      - Microsoft Hyper-V: scarica, distribuisci e configura la macchina virtuale gateway utilizzando Microsoft Hyper-V.
      - Linux KVM: scarica, distribuisci e configura la macchina virtuale gateway utilizzando Linux Kernel-based Virtual Machine (KVM).
      - Nutanix AHV: scarica, implementa e configura la macchina virtuale gateway utilizzando la macchina virtuale basata su kernel Linux (KVM). La stessa immagine funziona sia per gli ambienti hypervisor Linux KVM che per quelli Nutanix AHV.
      - Amazon EC2: configura e avvia un' EC2 istanza Amazon per ospitare il tuo gateway.
      - Dispositivo hardware: ordina un dispositivo hardware fisico dedicato da AWS cui ospitare il gateway.

   b. Per Conferma la configurazione del gateway, seleziona la casella di controllo per confermare di aver eseguito i passaggi di distribuzione per la piattaforma host scelta. Questo passaggio non è applicabile alla piattaforma host dell'appliance hardware.

6. Ora che il gateway è configurato, devi scegliere come connetterlo e comunicare AWS. Scegli Successivo per continuare.

Connect il tuo Amazon S3 File Gateway a AWS

Per connettere un nuovo S3 File Gateway a AWS

1. Se non l'hai già fatto, completa la procedura descritta in Configurazione di un Amazon S3 File Gateway. Al termine, scegli Avanti per aprire la AWS pagina Connect to nella Gateway di archiviazione AWS console.
2. Nella sezione Opzioni di connessione del gateway, per Opzioni di connessione, scegli come identificare il gateway verso AWS. Scegliere tra le seguenti opzioni:

   - Indirizzo IP: fornisci l'indirizzo IP del gateway nel campo corrispondente. Questo indirizzo IP deve essere pubblico o accessibile dall'interno della rete corrente e devi essere in grado di connetterti ad esso dal tuo browser web.

     Puoi ottenere l'indirizzo IP del gateway accedendo alla console locale del gateway dal tuo client hypervisor o copiandolo dalla pagina dei dettagli dell'istanza Amazon EC2 . Per ulteriori informazioni, consulta Ottenere l'indirizzo IP del gateway.
   - Chiave di attivazione: fornisci la chiave di attivazione per il gateway nel campo corrispondente. È possibile generare una chiave di attivazione utilizzando la console locale del gateway. Se l'indirizzo IP del gateway non è disponibile, scegli questa opzione.
3. Nella sezione Opzioni endpoint, procedi come segue:

   a. Per Service endpoint, scegli il tipo di endpoint con cui il gateway utilizzerà per comunicare. AWS Scegliere tra le seguenti opzioni:

      - Accessibile al pubblico: il gateway comunica tramite la rete AWS Internet pubblica. Se selezionate questa opzione, utilizzate la casella di controllo Endpoint abilitato FIPS per specificare se la connessione deve essere conforme ai Federal Information Processing Standards (FIPS).

        > **Note**
        >
        > Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint conforme a

FIPS. Per ulteriori informazioni, consulta Federal Information Processing Standard (FIPS) 140-2.
L'endpoint del servizio FIPS è disponibile solo in alcune regioni. AWS Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.

- VPC ospitato: il gateway comunica AWS tramite una connessione privata con il cloud privato virtuale (VPC), che consente di controllare le impostazioni di rete. Se si seleziona questa opzione, è necessario specificare un endpoint VPC esistente scegliendo il relativo ID endpoint VPC dall'elenco a discesa. Puoi anche fornire il nome o l'indirizzo IP del suo endpoint VPC Domain Name System (DNS).

> **Note**
>
> Per specificare un endpoint VPC che appartiene a un dispositivo Account AWS diverso da quello attualmente utilizzato per creare il gateway, è necessario fornire il nome DNS o l'indirizzo IP.

b. Per la versione IP, scegli la versione del protocollo e l'endpoint con cui il gateway utilizzerà per comunicare. AWS

> **Note**
>
> L'indirizzo IP del gateway deve corrispondere alla versione IP specificata qui. Gli endpoint dual-stack accettano IPv6 connessioni IPv4 e comunicano con il gateway solo utilizzando la versione IP selezionata.

4. Ora che hai scelto la modalità di connessione del gateway AWS, devi attivare il gateway. Scegli Successivo per continuare.

Rivedi le impostazioni e attiva il tuo Amazon S3 File Gateway

Per rivedere le impostazioni e attivare un nuovo S3 File Gateway

1. Se non l'hai già fatto, completa le procedure descritte nei seguenti argomenti:

   - Configurazione di un Amazon S3 File Gateway
   - Connect il tuo Amazon S3 File Gateway a AWS

Al termine, scegli Avanti per aprire la pagina di revisione e attivazione nella Gateway di archiviazione AWS console.

2. Rivedi i dettagli iniziali del gateway per ogni sezione della pagina.
3. Se una sezione contiene errori, scegli Modifica per tornare alla pagina delle impostazioni corrispondente e apportare modifiche.

> **Important**
>
> Non è possibile modificare le opzioni o le impostazioni di connessione del gateway dopo l'attivazione del gateway.

4. Dopo aver attivato il gateway, è necessario eseguire la prima configurazione per allocare i dischi di archiviazione locali e configurare la registrazione. Scegli Successivo per continuare.

Configura il tuo Amazon S3 File Gateway

Per eseguire la prima configurazione su un nuovo S3 File Gateway

1. Se non l'hai già fatto, completa le procedure descritte nei seguenti argomenti:

   - Configurazione di un Amazon S3 File Gateway
   - Connect il tuo Amazon S3 File Gateway a AWS
   - Rivedi le impostazioni e attiva il tuo Amazon S3 File Gateway

   Al termine, scegli Avanti per aprire la pagina Configure gateway nella Gateway di archiviazione AWS console.
2. Nella sezione Configura archiviazione, utilizza gli elenchi a discesa per allocare almeno un disco locale con almeno 150 gibibyte (GiB) di capacità alla cache. I dischi locali elencati in questa sezione corrispondono allo spazio di archiviazione fisico fornito sulla piattaforma host.
3. Nella sezione dei gruppi di CloudWatch log, scegli come configurare Amazon CloudWatch Logs per monitorare lo stato del tuo gateway. Scegliere tra le seguenti opzioni:

   - Crea un nuovo gruppo di log: configura un nuovo gruppo di log per monitorare il tuo gateway.
   - Usa un gruppo di log esistente: scegli un gruppo di log esistente dall'elenco a discesa corrispondente.

- Disattiva la registrazione: non utilizzare Amazon CloudWatch Logs per monitorare il gateway.

> **Note**
>
> Per ricevere i log di integrità dello Storage Gateway, nella politica delle risorse del gruppo di log devono essere presenti le seguenti autorizzazioni. Sostituisci le *highlighted section* informazioni ResourceArn con il gruppo di log specifico per la tua distribuzione.
>
> ```
> "Sid": "AWSLogDeliveryWrite20150319",
>       "Effect": "Allow",
>       "Principal": {
>         "Service": [
>           "delivery.logs.amazonaws.com"
>         ]
>       },
>       "Action": [
>         "logs:CreateLogStream",
>         "logs:PutLogEvents"
>       ],
>       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
> ```
>
> L'elemento «Resource» è richiesto solo se si desidera che le autorizzazioni si applichino esplicitamente a un singolo gruppo di log.

4. Nella sezione CloudWatch allarmi, scegli come configurare gli CloudWatch allarmi Amazon per avvisarti quando le metriche del tuo gateway si discostano dai limiti definiti. Scegliere tra le seguenti opzioni:

   - Crea allarmi consigliati da Storage Gateway: crea automaticamente tutti gli allarmi consigliati quando CloudWatch viene creato il gateway. Per ulteriori informazioni sugli allarmi consigliati, vedere Comprensione degli allarmi. CloudWatch

   > **Note**
   >
   > Questa funzionalità richiede le autorizzazioni relative alle CloudWatch policy, che non vengono concesse automaticamente come parte della policy di accesso completo preconfigurata di Storage Gateway. Assicurati che la tua politica di sicurezza conceda le seguenti autorizzazioni prima di tentare di creare allarmi consigliati: CloudWatch

- `cloudwatch:PutMetricAlarm`: creazione di allarmi
- `cloudwatch:DisableAlarmActions`: disattivazione delle azioni di allarme
- `cloudwatch:EnableAlarmActions`: attivazione delle azioni di allarme
- `cloudwatch:DeleteAlarms`: eliminazione di allarmi

- Crea un allarme personalizzato: configura un nuovo CloudWatch allarme per informarti sulle metriche del tuo gateway. Scegli Crea allarme per definire le metriche e specificare le azioni di allarme nella CloudWatch console Amazon. Per istruzioni, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.
- Nessun allarme: non ricevere CloudWatch notifiche sulle metriche del gateway.

5. (Facoltativo) Nella sezione Tag, scegli Aggiungi nuovo tag, quindi inserisci una coppia chiave-valore con distinzione tra maiuscole e minuscole per aiutarti a cercare e filtrare il gateway nelle pagine di elenco della console. Gateway di archiviazione AWS Ripeti questo passaggio per aggiungere quanti tag necessiti.
6. (Facoltativo) Nella sezione di configurazione Verify VMware High Availability, se il gateway è distribuito su un VMware host che fa parte di un cluster VMware High Availability (HA), scegli Verify VMware HA per verificare se la configurazione HA funziona correttamente.

   > **Note**
   >
   > Questa sezione viene visualizzata solo per i gateway in esecuzione sulla piattaforma VMware host.
   > Questo passaggio non è necessario per completare il processo di configurazione del gateway. È possibile testare la configurazione HA del gateway in qualsiasi momento. La verifica richiede alcuni minuti e riavvia la macchina virtuale (VM) Storage Gateway.

7. Scegli Configura per completare la creazione del gateway.

   Per verificare lo stato del nuovo gateway, cercalo nella pagina di panoramica del gateway della Gateway di archiviazione AWS console.

Ora che hai creato il gateway, devi creare una condivisione di file da utilizzare. Per istruzioni, consulta Creare una condivisione di file.

Attivazione di un gateway in un cloud privato virtuale

È possibile creare una connessione privata tra l'applicazione gateway on-premise e l'infrastruttura di archiviazione basata sul cloud. È possibile utilizzare questa connessione per attivare il gateway e configurarlo per trasferire dati ai servizi AWS di archiviazione senza comunicare sulla rete Internet pubblica. Utilizzando il servizio Amazon VPC, puoi avviare AWS risorse, inclusi endpoint di interfaccia di rete privata, in un cloud privato virtuale (VPC) personalizzato. Un VPC fornisce il controllo delle impostazioni di rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per ulteriori informazioni su VPCs, consulta Cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC.

Per attivare il gateway in un VPC, utilizza la console Amazon VPC per creare un endpoint VPC per Storage Gateway, crea un endpoint VPC per Storage Gateway e attivi il gateway. Per ulteriori informazioni, consulta Connect your Amazon S3 File Gateway to AWS Connect your a. AWS

Per configurare il tuo S3 File Gateway per il trasferimento di dati tramite il VPC, devi creare un endpoint VPC separato per Amazon S3, quindi specificare questo endpoint VPC quando crei condivisioni di file per il gateway.

> **Note**
>
> Devi attivare il gateway nella stessa regione in cui crei l'endpoint VPC per Storage Gateway e lo storage Amazon S3 che configuri per la condivisione di file deve trovarsi nella stessa regione in cui crei l'endpoint VPC per Amazon S3.

Crea un endpoint VPC per Storage Gateway

Per creare un endpoint VPC, attenersi alle istruzioni seguenti. Se disponi già di un endpoint VPC per Storage Gateway, puoi utilizzarlo.

Per creare un endpoint VPC per Storage Gateway

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. Nel riquadro di navigazione, selezionare Endpoint e scegliere Create Endpoint (Crea endpoint).
3. Nella pagina Crea endpoint, scegliere Servizi AWS per Categoria del servizio.

4. Per Service Name (Nome del servizio), selezionare `com.amazonaws.region.storagegateway`. Ad esempio, `com.amazonaws.us-east-2.storagegateway`.
5. Per VPC, scegliere il VPC e annotare le zone di disponibilità e le sottoreti.
6. Verifica che l'opzione Abilita nome DNS non sia selezionata.
7. Per Gruppo di sicurezza, scegliere il gruppo di sicurezza che si desidera utilizzare per il VPC. È possibile accettare il gruppo di sicurezza predefinito. Verificare che tutte le seguenti porte TCP siano consentite nel gruppo di sicurezza:

   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Seleziona Crea endpoint. Lo stato iniziale dell'endpoint è pending (in sospeso). Quando l'endpoint viene creato, prendere nota dell'ID dell'endpoint VPC appena creato.
9. Quando l'endpoint viene creato, scegliere Endpoint quindi il nuovo endpoint VPC.
10. Nella scheda Dettagli dell'endpoint del gateway di archiviazione selezionato, in Nomi DNS, utilizza il primo nome DNS che non specifica una zona di disponibilità. Il nome DNS dovrebbe essere simile al seguente esempio: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ora che hai un endpoint VPC, puoi creare e attivare il tuo gateway. Per ulteriori informazioni, consulta Creare e attivare un Amazon S3 File Gateway Gateway.

Per informazioni su come ottenere una chiave di attivazione, consulta Ottenere una chiave di attivazione per il gateway .

> **Important**
>
> Per configurare il tuo S3 File Gateway per il trasferimento di dati tramite il VPC, devi creare un endpoint VPC separato per Amazon S3, quindi specificare questo endpoint VPC quando crei condivisioni di file per il gateway.

Per fare ciò, segui gli stessi passaggi mostrati sopra, ma scegli Service Name, quindi seleziona `com.amazonaws.region.s3` la tabella di routing a cui desideri associare l'endpoint S3 anziché il gruppo. subnet/security Per istruzioni, consulta Creazione di un endpoint gateway.

Creazione di una condivisione file

In questa sezione, puoi trovare le istruzioni su come creare una condivisione di file a cui sia possibile accedere utilizzando il protocollo Network File System (NFS) o il Server Message Block (SMB).

Quando si crea una condivisione NFS, chiunque abbia accesso al server NFS può accedere alla condivisione di file NFS per impostazione predefinita. È possibile limitare l'accesso ai client in base all'indirizzo IP.

Quando si crea una condivisione di file SMB, è possibile utilizzare una delle tre modalità di autenticazione:

- Una condivisione di file con accesso a Microsoft Active Directory (AD). Qualsiasi utente Microsoft AD autenticato ottiene l'accesso a questo tipo di condivisione di file.
- Una condivisione di file SMB con accesso limitato. L'accesso è consentito solo a determinati utenti e gruppi di dominio specificati (tramite un elenco consentito). È inoltre possibile negare l'accesso a utenti e gruppi (tramite un elenco di utenti non autorizzati).
- Una condivisione di file SMB con accesso da ospite. Qualsiasi utente in grado di fornire la password dell'utente ospite ha accesso a questa condivisione di file.

> **Note**
>
> Le condivisioni di file esportate tramite il gateway per le condivisioni di file NFS supportano le autorizzazioni POSIX. Per le condivisioni di file SMB, è possibile utilizzare gli elenchi di controllo degli accessi (ACLs) per gestire le autorizzazioni su file e cartelle nella condivisione di file. Per ulteriori informazioni, consulta Utilizzo di Windows ACLs per limitare l'accesso alla condivisione di file SMB.

Un File Gateway può ospitare una o più condivisioni di file di diversi tipi. È possibile avere più condivisioni di file NFS e SMB su un File Gateway.

> **Important**
>
> Per creare una condivisione di file, un File Gateway richiede l'attivazione AWS Security Token Service ()AWS STS. Se AWS STS non è attivato nel punto in Regione AWS cui crei il File Gateway, attivalo. Per informazioni su come eseguire l'attivazione AWS STS, consulta

Attivazione e disattivazione AWS Security Token Service in una AWS regione nella Guida per l'AWS Identity and Access Management utente.

Argomenti

- Evitare costi imprevisti durante il caricamento dei dati del gateway
- Crittografa gli oggetti archiviati da File Gateway in Amazon S3
- Creare una condivisione di file NFS
- Creare una condivisione di file SMB

Evitare costi imprevisti durante il caricamento dei dati del gateway

Quando un file viene scritto su File Gateway da un client NFS, File Gateway carica i dati del file su Amazon S3 seguiti dai relativi metadati. Il caricamento dei dati del file crea un oggetto S3 e il caricamento dei metadati del file aggiorna i metadati per l'oggetto S3. Questo processo crea una versione aggiuntiva dell'oggetto. Se il controllo delle versioni S3 è attivato, entrambe le versioni vengono archiviate.

Se modifichi i metadati di un file archiviato nel File Gateway, viene creato un nuovo oggetto S3 che sostituisce l'oggetto S3 esistente. Questo comportamento è diverso dalla modifica di un file in un file system, in cui la modifica di un file non comporta la creazione di un nuovo file. Testa tutte le operazioni sui file che intendi utilizzare con AWS Storage Gateway in modo da capire come ogni operazione sui file interagisce con lo storage Amazon S3.

Valuta attentamente l'uso del controllo delle versioni di S3 e della replica tra regioni (CRR) in Amazon S3 quando carichi dati dal tuo File Gateway. Il caricamento di file da File Gateway ad Amazon S3 quando il controllo delle versioni S3 è attivato in genere genera più di una versione di un oggetto S3.

Alcuni flussi di lavoro che coinvolgono file di grandi dimensioni e schemi di scrittura dei file, come i caricamenti di file eseguiti in più fasi, possono aumentare il numero di versioni di oggetti S3 archiviate. Se la cache di File Gateway deve liberare spazio a causa delle elevate velocità di scrittura dei file, potrebbero essere create più versioni di oggetti S3. Questi scenari aumentano lo storage S3 se S3 Versioning è attivato e aumentano i costi di trasferimento associati al CRR. Testa tutte le operazioni sui file che intendi utilizzare con Storage Gateway in modo da capire come ogni operazione sui file interagisce con lo storage Amazon S3.

L'utilizzo dell'utilità Rsync con File Gateway comporta la creazione di file temporanei nella cache e la creazione di oggetti S3 temporanei in Amazon S3. Questa situazione comporta costi di eliminazione anticipata nella classe di storage S3 Standard-Infrequent Access (S3 Standard-IA).

Crittografa gli oggetti archiviati da File Gateway in Amazon S3

S3 File Gateway supporta i seguenti metodi di crittografia lato server per i dati archiviati in Amazon S3:

- SSE-S3: per impostazione predefinita, tutti i nuovi oggetti caricati nei bucket Amazon S3 utilizzano la crittografia lato server con chiavi gestite di Amazon S3. Per ulteriori informazioni, consulta Usare la crittografia lato server con le chiavi gestite di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.
- SSE-KMS: puoi configurare la condivisione di file per utilizzare la crittografia lato server con () chiavi gestite. AWS Key Management Service AWS KMS AWS KMS è un servizio che combina hardware e software sicuri e ad alta disponibilità per fornire un sistema di gestione delle chiavi scalabile per il cloud. Per ulteriori informazioni, consulta Cos'è il servizio di gestione delle AWS chiavi? nella Guida per gli AWS Key Management Service sviluppatori.
- DSSE-KMS: la crittografia lato server a doppio livello con AWS KMS chiavi applica due livelli di crittografia agli oggetti quando vengono caricati su Amazon S3. Questo aiuta a soddisfare gli standard di conformità per la crittografia multistrato. Per ulteriori informazioni, consulta Uso della crittografia lato server a doppio livello con chiavi AWS KMS nella Guida per l'utente di Amazon Simple Storage Service.

> **Note**
>
> Sono previsti costi aggiuntivi per l'utilizzo di DSSE-KMS e delle chiavi. AWS KMS Per ulteriori informazioni, consultare Prezzi di AWS KMS.

È possibile specificare un metodo di crittografia quando si crea una nuova condivisione di file utilizzando la console Storage Gateway o l'API Storage Gateway. Per le procedure della console, vedere Crea una condivisione di file NFS con una configurazione personalizzata oCrea una condivisione di file SMB con una configurazione personalizzata. Per informazioni sui comandi API corrispondenti, vedere Create NFSFile Share o Create SMBFile Share nello AWS Storage Gateway API Reference.

È inoltre possibile aggiornare le impostazioni di crittografia per una condivisione di file esistente utilizzando la console Storage Gateway o l'API Storage Gateway. Per la procedura della console, vedereModifica il metodo di crittografia lato server per una condivisione di file esistente. Per informazioni sui comandi API corrispondenti, vedere Update NFSFile Share o Update SMBFile Share nello AWS Storage Gateway API Reference.

> **Note**
>
> Dopo aver aggiornato il metodo di crittografia, il gateway utilizza il nuovo metodo per tutti i nuovi oggetti che crea in Amazon S3 e per tutti gli oggetti archiviati che aggiornerà o modificherà in futuro. Gli oggetti Amazon S3 esistenti riceveranno il nuovo metodo di crittografia solo se vengono aggiornati o modificati dal gateway.

> **Important**
>
> Assicurati che la condivisione di file utilizzi lo stesso tipo di crittografia del bucket Amazon S3 in cui archivia i dati.
> Se configuri File Gateway per utilizzare SSE-KMS o DSSE-KMS per la crittografia, devi aggiungere manualmente,, `kms:Encrypt` `kms:Decrypt` `kms:ReEncrypt*` `kms:GenerateDataKey`, e le `kms:DescribeKey` autorizzazioni al ruolo IAM associato alla condivisione di file. Per ulteriori informazioni, consulta Using Identity-Based Policies (IAM Policies) for Storage Gateway.

Creare una condivisione di file NFS

Il protocollo Network File System (NFS) è un protocollo di condivisione di file con stato per sistemi basati su UNIX. Quando un client abilitato per NFS e un server NFS comunicano, il client richiede un file o una directory dal server utilizzando chiamate di procedura remota (RPC). Il server verifica che il file o la directory siano disponibili e che il client disponga delle autorizzazioni di accesso richieste. Il server monta quindi il file o la directory in remoto sul client e condivide l'accesso tramite una connessione virtuale. Per le operazioni client, NFS rende l'utilizzo del file del server remoto simile all'accesso a un file locale.

> **Note**
>
> Il protocollo NFS supporta un massimo di 16 gruppi per utente. Gli utenti potrebbero avere problemi a montare le condivisioni di file NFS se appartengono a più di 16 gruppi. Per evitare problemi di montaggio, assicuratevi che gli utenti siano membri di 16 o meno gruppi quando accedono alle condivisioni di file NFS.

I seguenti argomenti spiegano vari metodi per creare una condivisione di file NFS per File Gateway:

Indice

- Creare una condivisione di file NFS utilizzando la configurazione predefinita
  - Impostazioni di configurazione predefinite per le condivisioni di file NFS
- Crea una condivisione di file NFS con una configurazione personalizzata

Creare una condivisione di file NFS utilizzando la configurazione predefinita

Questa sezione spiega come creare una nuova condivisione di file Network File System (NFS) utilizzando impostazioni preconfigurate preconfigurate. Utilizzate questo metodo per distribuzioni di base, uso personale, test o per distribuire rapidamente più condivisioni di file che intendete modificare e personalizzare in un secondo momento. Per un elenco delle impostazioni predefinite per le condivisioni di file create utilizzando questa procedura, vedere Impostazioni di configurazione predefinite per le condivisioni di file NFS. Se hai bisogno di un controllo più granulare o desideri utilizzare impostazioni avanzate per la condivisione di file, vedi Creare una condivisione di file NFS utilizzando una configurazione personalizzata.

> **Note**
>
> Se devi connettere la tua condivisione di file ad Amazon S3 tramite un Virtual Private Cloud (VPC), devi seguire la procedura di configurazione personalizzata. Non puoi modificare le impostazioni VPC per una condivisione di file dopo averla creata.

> **Important**
>
> L'utilizzo di S3 Versioning, Cross-Region Replication o dell'utilità Rsync durante il caricamento di dati da un File Gateway può avere implicazioni significative in termini di costi.

Per ulteriori informazioni, consulta Evitare costi imprevisti durante il caricamento di dati da File Gateway.

Per creare una condivisione di file NFS utilizzando la configurazione predefinita:

1. Apri la console AWS Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/ e scegli Condivisioni di file dal riquadro di navigazione a sinistra.
2. Scegliere Create file share (Crea condivisione file).
3. Per Gateway, scegli il tuo Amazon S3 File Gateway dall'elenco.
4. Per il protocollo di condivisione dei file, scegli NFS.
5. Per il bucket S3, esegui una delle seguenti operazioni:
   - Scegli un bucket Amazon S3 esistente nel tuo account dall'elenco a discesa.
   - Scegli Un bucket in un altro account dall'elenco a discesa, quindi inserisci il nome del bucket in Cross-account bucket name.
   - Scegli Crea nuovo bucket S3, quindi scegli Regione AWS dove si trova l'endpoint Amazon S3 per il tuo nuovo bucket e inserisci un nome di bucket S3 univoco. Al termine, scegli Crea bucket S3.

     Per informazioni sulla creazione di un nuovo bucket, vedi Come si crea un bucket S3? nella Guida per l'utente di Amazon S3.

   > **Note**
   >
   > S3 File Gateway non supporta i bucket Amazon S3 con periodi `.` () nel nome del bucket. Assicurati che il nome del bucket sia conforme alle regole per la denominazione dei bucket in Amazon S3. Per ulteriori informazioni, consulta le Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

6. Controlla le impostazioni in Configurazione predefinita, quindi scegli Crea condivisione file per creare la tua nuova condivisione di file NFS utilizzando la configurazione predefinita.

Dopo aver creato la condivisione di file NFS, è possibile visualizzarne le impostazioni di configurazione nella console AWS Storage Gateway nella scheda Dettagli della condivisione di file.

Per informazioni sul montaggio della condivisione di file, vedi Installare la condivisione di file NFS sul client.

Impostazioni di configurazione predefinite per le condivisioni di file NFS

Le seguenti impostazioni si applicano a tutte le nuove condivisioni di file NFS create utilizzando la configurazione predefinita. Dopo aver creato una condivisione di file, è possibile selezionarla dalla pagina Condivisioni di file nella console di AWS Storage Gateway per visualizzare i dettagli sulla sua configurazione.

> **Important**
>
> La configurazione predefinita della condivisione di file NFS fornisce il controllo completo dei file e le autorizzazioni di accesso al proprietario del bucket S3 mappato alla condivisione di file, anche se il bucket è di proprietà di un account diverso. AWS Per ulteriori informazioni sull'utilizzo della condivisione di file per accedere agli oggetti in un bucket di proprietà di un altro account, consulta. Utilizzo di una condivisione di file per l'accesso a più account

Impostazione	Valore predefinito	Note
Ubicazione Amazon S3	La condivisione di file si connette direttamente al bucket Amazon S3 e ha lo stesso nome del bucket. Il gateway utilizza questo bucket per archiviare e recuperare file.	Il nome non include un prefisso.
AWS PrivateLink per S3	La condivisione di file non si connette ad Amazon S3 tramite un endpoint di interfacc ia nel tuo cloud privato virtuale (VPC).	
Notifica di caricamento dei file	Disattivata	

Impostazione	Valore predefinito	Note
Classe di archiviazione per nuovi oggetti	Amazon S3 standard	Ciò consente di archiviare i dati degli oggetti a cui si accede di frequente in modo ridondante in più zone di disponibilità geograficamente separate. Per ulteriori informazioni sulla classe di Amazon S3 Standard storage, consulta Classi di storage per oggetti a cui si accede di frequente nella Amazon Simple Storage Service User Guide.
Encryption (Crittografia)	Crittografia lato server con chiavi gestite S3 (SSE-S3)	Tutti gli oggetti Amazon S3 caricati, aggiornati o modificati da S3 File Gateway sono crittografati per impostazione predefinita con crittografia lato server utilizzando chiavi gestite di Amazon S3.

Impostazione	Valore predefinito	Note
Metadati degli oggetti	Indovina il tipo MIME	Ciò consente a Storage Gateway di indovinare il tipo MIME (Multipurpose Internet Mail Extension) per gli oggetti caricati in base alle estensioni di file. Questa opzione richiede che le liste di controllo degli accessi (ACLs) siano attivate per il bucket Amazon S3 associato alla condivisione di file. Se sono ACLs disattivata, la condivisione di file non può accedere al bucket Amazon S3 e rimane nello stato Non disponibile indefinitamente.
Abilita i pagamenti del richiedente	Disattivata	Per ulteriori informazioni, consulta Bucket con pagamento a carico del richiedente.
Log di verifica	Disattivata	La registrazione a un Amazon CloudWatch gruppo è disattivata per impostazione predefinita.

Impostazione	Valore predefinito	Note
Accesso al tuo bucket S3	Crea un nuovo ruolo IAM	L'opzione predefinita consente a File Gateway di creare un nuovo ruolo e accesso IAM politica per tuo conto. L'accesso è consentito a tutti i client NFS. Per informazioni sui supporti Client NFS, vedereClient NFS e SMB supportati per File Gateway.
Opzioni di montaggio	• Livello di squash: zucca con radici • Esporta come: lettura-scrittura	Il valore predefinito di Squash level significa che accesso per il telecomando superuser (root) è mappato su User Identifier (UID) (65534) e Group Identifier (GID) (65534).
Impostazioni predefinite dei metadati dei file	• Autorizzazioni di directory: 0777 • Autorizzazioni relative ai file — 0666 • Identificatore utente (UID) — 65534 • Identificatore di gruppo (GID) — 65534	

Crea una condivisione di file NFS con una configurazione personalizzata

Utilizzare la procedura seguente per creare una condivisione di file Network File System (NFS) con una configurazione personalizzata. Per creare una condivisione di file NFS utilizzando le impostazioni di configurazione predefinite, vedere Creare una condivisione di file NFS utilizzando la configurazione predefinita.

> **Important**
>
> L'utilizzo di S3 Versioning, Cross-Region Replication o dell'utilità Rsync durante il caricamento di dati da un File Gateway può avere implicazioni significative in termini di costi. Per ulteriori informazioni, consulta Evitare costi imprevisti durante il caricamento di dati da File Gateway.

Per creare una condivisione di file NFS con impostazioni personalizzate

1. Apri la console AWS Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/ e scegli Condivisioni di file dal riquadro di navigazione a sinistra.
2. Scegliere Create file share (Crea condivisione file).
3. Scegli Personalizza la configurazione. Per ora puoi ignorare gli altri campi di questa pagina. Nei passaggi successivi ti verrà richiesto di configurare le impostazioni del gateway, del protocollo e dello storage.
4. Per Gateway, scegli Amazon S3 File Gateway per la tua nuova condivisione di file dall'elenco a discesa.
5. Per il gruppo di CloudWatch log, scegli una delle seguenti opzioni dall'elenco a discesa:

   - Per disattivare la registrazione per questa condivisione di file, scegli Disabilita registrazione.
   - Per creare automaticamente un nuovo gruppo di log per questa condivisione di file, scegliere Creato da Storage Gateway.
   - Per inviare notifiche sullo stato e sulle risorse per questa condivisione di file a un gruppo di log esistente, scegli il gruppo desiderato dall'elenco.

   Per ulteriori informazioni sui log di controllo, consulta Understanding S3 File Gateway audit logs.
6. (Facoltativo) In Tag - Facoltativo, scegli Aggiungi nuovo tag, quindi inserisci una chiave e un valore per la condivisione di file.

   Un tag è una coppia chiave-valore con distinzione tra maiuscole e minuscole che consente di classificare le risorse dello Storage Gateway. L'aggiunta di tag può semplificare il filtraggio e la ricerca della condivisione di file. Puoi ripetere questo passaggio per aggiungere fino a 50 tag.

   Al termine, scegli Avanti.

7. Per il bucket S3, esegui una delle seguenti operazioni per specificare dove la condivisione di file archivierà e recupererà i file:

   - Per connettere la condivisione di file direttamente a un bucket S3 esistente nel tuo account Amazon Web Services, scegli il nome del bucket dall'elenco a discesa.
   - Per connettere la condivisione di file a un bucket S3 esistente di proprietà di un account Amazon Web Services diverso da quello che usi per creare la condivisione di file, scegli Un bucket in un altro account dall'elenco a discesa, quindi inserisci il nome del bucket Cross-account.
   - Per connettere la condivisione di file a un nuovo bucket S3, scegli Crea un nuovo bucket S3, quindi scegli la regione in cui si trova l'endpoint Amazon S3 per il nuovo bucket e inserisci un nome di bucket S3 univoco. Al termine, scegli Crea bucket S3. Per ulteriori informazioni sulla creazione di nuovi bucket, vedi Come si crea un bucket S3? nella Guida per l'utente di Amazon S3.
   - Per connettere la condivisione di file a un bucket S3 utilizzando il nome di un punto di accesso, scegli il nome del punto di accesso Amazon S3 dall'elenco a discesa, quindi inserisci il nome del punto di accesso. Se devi creare un nuovo punto di accesso, puoi scegliere Crea un punto di accesso S3. Per ulteriori istruzioni, consulta Creazione di un punto di accesso nella Guida per l'utente di Amazon S3. Per ulteriori informazioni sui punti di accesso, consulta Gestire l'accesso ai dati con i punti di accesso Amazon S3 e Delegare il controllo degli accessi ai punti di accesso nella Amazon S3 User Guide.
   - Per connettere la condivisione di file a un bucket S3 utilizzando un alias del punto di accesso, scegli l'alias del punto di accesso Amazon S3 dall'elenco a discesa, quindi inserisci l'alias del punto di accesso. Se devi creare un nuovo punto di accesso, puoi scegliere Crea un punto di accesso S3. Per ulteriori istruzioni, consulta Creazione di un punto di accesso nella Guida per l'utente di Amazon S3. Per ulteriori informazioni sugli alias dei punti di accesso, consulta Using a bucket alias for your access point nella Amazon S3 User Guide.

   > **Note**
   >
   > Ogni condivisione di file può connettersi solo a un bucket S3, ma più condivisioni di file possono connettersi allo stesso bucket. Se connetti più di una condivisione di file allo stesso bucket, devi configurare ogni condivisione di file in modo che utilizzi un prefisso di bucket S3 univoco e non sovrapposto per evitare conflitti. read/write
   > S3 File Gateway non supporta i bucket Amazon S3 con periodi `.` () nel nome del bucket.

Assicurati che il nome del bucket sia conforme alle regole per la denominazione dei bucket in Amazon S3. Per ulteriori informazioni, consulta le Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

8. (Facoltativo) Per il prefisso del bucket S3, inserisci un prefisso per la condivisione di file da applicare agli oggetti che crea in Amazon S3. I prefissi sono un modo per organizzare i dati in S3, in modo simile alle directory nelle strutture di file tradizionali. Per ulteriori informazioni, consulta Organization objects using prefixes nella Amazon S3 User Guide.

   Note

   - Se connetti più di una condivisione di file allo stesso bucket, devi configurare ogni condivisione di file in modo che utilizzi un prefisso unico e non sovrapposto per evitare conflitti. read/write
   - Il prefisso deve terminare con una barra (/).
   - Dopo aver creato la condivisione di file, il prefisso non può essere modificato o eliminato.

9. Per Regione, scegli Regione AWS dove si trova l'endpoint S3 per il tuo bucket dall'elenco a discesa. Questo campo viene visualizzato solo quando specifichi un punto di accesso o un bucket in un altro account per il bucket S3.
10. Per Classe di archiviazione per nuovi oggetti, scegli una classe di archiviazione dall'elenco a discesa. Per ulteriori informazioni sulle classi di archiviazione, consulta Utilizzo delle classi di archiviazione con un File Gateway.
11. Per IAM Role, esegui una delle seguenti operazioni per configurare un ruolo IAM per la condivisione di file:

    - Per creare automaticamente un nuovo ruolo IAM con le autorizzazioni necessarie per il corretto funzionamento della condivisione di file, scegli Created by Storage Gateway dall'elenco a discesa.
    - Per utilizzare un ruolo IAM esistente, scegli il nome del ruolo dall'elenco a discesa.
    - Per creare un nuovo ruolo IAM, scegli Crea un ruolo. Per ulteriori istruzioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l' AWS Identity and Access Management utente.

Per ulteriori informazioni su come i ruoli IAM controllano l'accesso tra la condivisione di file e il bucket S3, consulta Garantire l'accesso a un bucket Amazon S3.

12. Per Link privato, procedi come segue solo se devi configurare la condivisione di file con cui comunicare AWS utilizzando un endpoint privato in un Virtual Private Cloud (VPC). In caso contrario, puoi ignorare questo passaggio. Per ulteriori informazioni, consulta Cos'è? AWS PrivateLink nella AWS PrivateLink Guida.

    a. Seleziona Usa endpoint VPC.

    b. Per Identify VPC endpoint by, esegui una delle seguenti operazioni:

    - Seleziona ID endpoint VPC, quindi scegli l'endpoint che desideri utilizzare dall'elenco a discesa degli endpoint VPC.
    - Seleziona il nome DNS, quindi inserisci il nome DNS dell'endpoint che desideri utilizzare.

13. Per la crittografia, scegli il tipo di crittografia lato server che la condivisione di file utilizzerà per i dati archiviati in Amazon S3:

- Per utilizzare la crittografia lato server gestita con Amazon S3 (SSE-S3), scegli S3 Managed Keys (SSE-S3).

  Per ulteriori informazioni, consulta Usare la crittografia lato server con le chiavi gestite di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

- Per utilizzare la crittografia lato server gestita con AWS Key Management Service (SSE-KMS), scegli KMS-Managed Keys (SSE-KMS). Per la chiave KMS primaria, scegli una chiave KMS esistente o scegli Crea una nuova chiave AWS KMS per creare una nuova chiave KMS nella console del servizio di gestione delle chiavi (). AWS AWS KMS

  Per ulteriori informazioni su AWS KMS, consulta Cos'è AWS il servizio di gestione delle chiavi? nella Guida per gli AWS Key Management Service sviluppatori.

- Per utilizzare la crittografia lato server a doppio livello gestita con AWS Key Management Service (DSSE-KMS), scegli la crittografia lato server a doppio livello con chiavi (DSSE-KMS). AWS Key Management Service Per la chiave KMS primaria, scegli una chiave KMS esistente o scegli Crea una nuova chiave AWS KMS per creare una nuova chiave KMS nella console Key Management Service (). AWS AWS KMS

  Per ulteriori informazioni su DSSE-KMS, consulta Uso della crittografia lato server a doppio livello con chiavi AWS KMS nella Guida per l'utente di Amazon Simple Storage Service.

> **Note**
>
> Sono previsti costi aggiuntivi per l'utilizzo di DSSE-KMS e delle chiavi. AWS KMS Per ulteriori informazioni, consulta Prezzi di AWS KMS.
> Per specificare una AWS KMS chiave con un alias non presente nell'elenco o per utilizzare una AWS KMS chiave di un AWS account diverso, è necessario utilizzare il. AWS Command Line Interface Le chiavi KMS asimmetriche non sono supportate. Per ulteriori informazioni, vedere Create NFSFile Share nello AWS Storage Gateway API Reference.

> **Important**
>
> Assicurati che la condivisione di file utilizzi lo stesso tipo di crittografia del bucket Amazon S3 in cui archivia i dati.

14. Per i tipi Guess MIME, selezionare il tipo MIME multimediale Guess per consentire a Storage Gateway di indovinare il tipo di file per gli oggetti caricati in base alle relative estensioni di file.
15. Per il nome della condivisione di file, inserisci un nome per la condivisione di file.

> **Note**
>
> Un nome di condivisione di file NFS valido può contenere solo i seguenti caratteri: a `A` - `zZ`, `0` -9,, `-`.`.`, e`_`.

16. Per Eventi di caricamento, seleziona Registra un evento quando un file viene caricato correttamente dal gateway se desideri che il gateway registri gli eventi di CloudWatch registro quando carica correttamente i file su Amazon S3. Il ritardo di notifica controlla il ritardo minimo tra l'operazione di scrittura del client più recente e la generazione della notifica di `ObjectUploaded` registro. Poiché i client possono eseguire molte piccole scritture su file in breve tempo, consigliamo di impostare questo parametro il più a lungo possibile per evitare di generare più notifiche per lo stesso file in rapida successione. Per ulteriori informazioni, consulta Ricevere una notifica di caricamento di file.

> **Note**
>
> Questa impostazione non ha effetto sulla tempistica del caricamento dell'oggetto su S3, ma solo sulla tempistica della notifica.
> Questa impostazione non ha lo scopo di specificare l'ora esatta in cui verrà inviata la notifica. In alcuni casi, il gateway potrebbe richiedere un tempo di ritardo superiore a quello specificato per generare e inviare notifiche.

Al termine, scegli Avanti.

17.

18. Per Protocollo di condivisione file, scegli NFS.
19. Per l'accesso tramite client, effettuate una delle seguenti operazioni per specificare quali client NFS possono accedere alla condivisione di file:

    - Per accettare tutte le connessioni client in entrata, selezionate Tutti i client NFS.
    - Per accettare connessioni client in entrata solo da indirizzi IP specifici, seleziona Client NFS specifici, quindi scegli Aggiungi un client. Per Client consentiti, specifica un indirizzo IP o un blocco CIDR valido da cui accettare le connessioni. Se devi specificare indirizzi IP aggiuntivi, scegli Aggiungi un altro client.

    > **Note**
    >
    > Ti consigliamo di configurare la limitazione dell'accesso alla condivisione di file utilizzando l'opzione Client NFS specifici. In caso contrario, qualsiasi client della rete può eseguire il montaggio sulla condivisione di file.

20. Per Tipo di accesso, seleziona una delle seguenti opzioni:

    - Per consentire ai client di leggere e scrivere file sulla condivisione di file, seleziona Lettura/scrittura.
    - Per consentire ai client di leggere i file ma non di scrivere nella condivisione di file, seleziona Sola lettura.

> **Note**
>
> Per le condivisioni di file montate su un client Microsoft Windows, se si sceglie Sola lettura, è possibile che venga visualizzato un messaggio relativo a un errore imprevisto che impedisce di creare la cartella. Ignorare questo messaggio.

21. Per Livello di accesso, scegli una delle seguenti opzioni:

    - Root squash (default) (Squash root - impostazione predefinita): l'accesso per il superuser remoto (root) è mappato a UID (65534) e GID (65534).
    - All squash (Squash completo): gli accessi di tutti gli utenti sono mappati all'ID utente (UID) (65534) e all'ID gruppo (GID) (65534).
    - No root squash (Nessuno squash root): il superuser remoto (root) riceve l'accesso come root.

22. (Facoltativo) Per l'aggiornamento automatico della cache da S3, scegli Imposta intervallo di aggiornamento della cache, quindi imposta il tempo in minuti o giorni per aggiornare la cache della condivisione di file utilizzando Time To Live (TTL). TTL è il periodo di tempo trascorso dall'ultimo aggiornamento. Trascorso l'intervallo TTL, l'accesso a una directory fa sì che File Gateway aggiorni i contenuti di quella directory dal bucket Amazon S3.

    > **Note**
    >
    > L'impostazione di questo valore in un periodo inferiore a 30 minuti può influire negativamente sulle prestazioni del gateway in situazioni in cui viene spesso creato o eliminato un numero elevato di oggetti Amazon S3.

23. Per le impostazioni predefinite dei metadati dei file, seleziona Modifica i metadati predefiniti per gli oggetti S3 che non sono stati creati o modificati dal gateway se desideri che il gateway applichi i metadati dei file (incluse le autorizzazioni Unix) agli oggetti preesistenti che rileva nel bucket S3. Specificate le autorizzazioni Directory, le autorizzazioni per i file, l'ID utente e l'ID di gruppo che desiderate applicare nei campi corrispondenti.
24. Per Proprietà e autorizzazioni dei file, seleziona Assegna al proprietario del bucket S3 la piena proprietà dei file creati dal gateway, incluse le autorizzazioni di lettura, scrittura, modifica ed eliminazione, se desideri che l' AWS account proprietario del bucket S3 abbia il pieno controllo di tutti gli oggetti scritti nel bucket dalla tua condivisione di file.

    Al termine, scegli Avanti.

25. Rivedi la configurazione della condivisione dei file. Scegliete Modifica per modificare le impostazioni di qualsiasi sezione che desiderate modificare. Al termine, scegli Create (Crea).

Dopo aver creato la condivisione di file NFS, è possibile visualizzarne le impostazioni di configurazione nella console AWS Storage Gateway nella scheda Dettagli della condivisione di file. Per istruzioni su come montare la condivisione di file, vedi Installare la condivisione di file NFS sul client.

Creare una condivisione di file SMB

Il protocollo Server Message Block (SMB) è profondamente integrato nella suite di prodotti Microsoft Windows e rimane il protocollo di condivisione file predefinito per i sistemi operativi Windows. Il processo di comunicazione client-server è simile a NFS ad alto livello, ma ci sono differenze in alcuni dettagli e nei meccanismi operativi. Ad esempio, in SMB, i file system non sono montati sul client SMB locale. Si accede invece a una condivisione di rete ospitata sul server SMB tramite un percorso di rete.

Gli argomenti di questa sezione spiegano vari metodi per creare una condivisione di file SMB per File Gateway.

Indice

- Creare una condivisione di file SMB utilizzando la configurazione predefinita
  - Impostazioni di configurazione predefinite per le condivisioni di file SMB
- Crea una condivisione di file SMB con una configurazione personalizzata

Creare una condivisione di file SMB utilizzando la configurazione predefinita

Questa sezione spiega come creare una nuova condivisione di file Server Message Block (SMB) utilizzando impostazioni preconfigurate preconfigurate. Utilizzate questo metodo per distribuzioni di base, uso personale, test o per distribuire rapidamente più condivisioni di file che intendete modificare e personalizzare in un secondo momento. Per un elenco delle impostazioni predefinite per le condivisioni di file create utilizzando questa procedura, consulta Impostazioni di configurazione predefinite per le condivisioni di file SMB. Se hai bisogno di un controllo più granulare o desideri utilizzare impostazioni avanzate per la condivisione di file, consulta Creare una condivisione di file SMB con una configurazione personalizzata.

> **Note**
>
> Se devi connettere la tua condivisione di file ad Amazon S3 tramite un Virtual Private Cloud (VPC), devi seguire la procedura di configurazione personalizzata. Non puoi modificare le impostazioni VPC per una condivisione di file dopo averla creata.

> **Important**
>
> L'utilizzo di S3 Versioning, Cross-Region Replication o dell'utilità Rsync durante il caricamento di dati da un File Gateway può avere implicazioni significative in termini di costi. Per ulteriori informazioni, consulta Evitare costi imprevisti durante il caricamento di dati da File Gateway.

Prerequisiti

Prima di creare la condivisione di file, procedi come segue:

- Configura le impostazioni di sicurezza SMB per il tuo File Gateway. Per istruzioni, consulta Impostazione di un livello di sicurezza per il gateway.
- Configura Microsoft Active Directory o l'accesso guest per l'autenticazione. Per istruzioni, consulta Utilizzo di Active Directory per autenticare gli utenti o Fornire l'accesso come ospite alla condivisione di file.
- Assicurati che le porte richieste siano aperte nel tuo gruppo di sicurezza. Per ulteriori informazioni, consulta Requisiti delle porte.

Per creare una condivisione di file SMB utilizzando la configurazione predefinita:

1. Apri la console AWS Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/ e scegli Condivisioni di file dal riquadro di navigazione a sinistra.
2. Scegliere Create file share (Crea condivisione file).
3. Per Gateway, scegli Amazon S3 File Gateway dall'elenco a discesa.
4. Per il protocollo di condivisione dei file, scegli SMB.
5. Per il bucket S3, esegui una delle seguenti operazioni:
   - Scegli un bucket Amazon S3 esistente nel tuo account dall'elenco a discesa.

- Scegli Un bucket in un altro account dall'elenco a discesa, quindi inserisci il nome del bucket in Cross-account bucket name.
- Scegli Crea nuovo bucket S3, quindi scegli Regione AWS dove si trova l'endpoint Amazon S3 per il tuo nuovo bucket e inserisci un nome di bucket S3 univoco. Al termine, scegli Crea bucket S3.

  Per informazioni sulla creazione di un nuovo bucket, vedi Come si crea un bucket S3? nella Guida per l'utente di Amazon S3.

> **Note**
>
> S3 File Gateway non supporta i bucket Amazon S3 con periodi `.` () nel nome del bucket. Assicurati che il nome del bucket sia conforme alle regole per la denominazione dei bucket in Amazon S3. Per ulteriori informazioni, consulta le Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

6. Autenticazione utente, scegli il metodo di autenticazione che desideri utilizzare dall'elenco a discesa:

- Per utilizzare Microsoft Active Directory aziendale o AWS Managed Microsoft AD per autenticare l'accesso degli utenti alla condivisione di file SMB, scegli Active Directory. Il gateway deve essere aggiunto a un dominio per utilizzare questo metodo. Per ulteriori informazioni, vedere Utilizzo di Active Directory per autenticare gli utenti.

> **Note**
>
> Per AWS Managed Microsoft AD utilizzarla con un EC2 gateway Amazon, devi creare l' EC2istanza Amazon nello stesso VPC di AWS Managed Microsoft AD, aggiungere il gruppo di `_workspaceMembers` sicurezza all' EC2 istanza Amazon e unirti al dominio AD utilizzando le credenziali di amministratore di. AWS Managed Microsoft AD
> Per ulteriori informazioni in merito AWS Managed Microsoft AD, consulta la Guida all'AWS Directory Service amministrazione.
> Per ulteriori informazioni su Amazon EC2, consulta la documentazione di Amazon Elastic Compute Cloud.

Se lo stato di accesso indica che il gateway è già aggiunto a un dominio Active Directory, procedi al passaggio successivo. In caso contrario, eseguire le seguenti operazioni:

1. Scegli Configura.
2. Per Dominio, inserisci il nome del dominio Active Directory a cui desideri aggiungere il gateway.
3. Inserisci il nome utente e la password che il gateway utilizzerà per accedere al dominio.
4. (Facoltativo) Per Unità organizzativa (OU), immettere l'unità organizzativa designata utilizzata da Active Directory per i nuovi oggetti del computer.
5. (Facoltativo) Per i controller di dominio (DC), immettete il nome del controller di dominio tramite il quale il gateway si connetterà ad Active Directory. Puoi lasciare vuoto questo campo per consentire al DNS di selezionare automaticamente un DC.
6. Scegli Iscriviti ad Active Directory.

> **Note**
>
> L'aggiunta a un dominio crea un account Active Directory nel contenitore predefinito (che non è un'unità organizzativa) utilizzando l'ID Gateway come nome dell'account (ad esempio, SGW-1234ADE). Non è possibile personalizzare il nome di questo account.
> Se l'ambiente Active Directory richiede la preconfigurazione degli account per facilitare il processo di aggiunta al dominio, è necessario creare questo account in anticipo.
> Se l'ambiente Active Directory dispone di un'unità organizzativa designata per i nuovi oggetti del computer, è necessario specificare tale unità organizzativa al momento dell'accesso al dominio.

- Per concedere l'accesso protetto da password a chiunque fornisca la password guest configurata, scegli Accesso ospite. Non è necessario che File Gateway faccia parte di un dominio Microsoft Active Directory per utilizzare questo metodo. Scegli Configura per specificare la tua password Guest, quindi scegli Salva.

7. Controlla le impostazioni in Configurazione predefinita, quindi scegli Crea condivisione file per creare la tua nuova condivisione di file SMB utilizzando la configurazione predefinita.

Dopo aver creato la condivisione di file SMB, è possibile visualizzarne le impostazioni di configurazione nella console AWS Storage Gateway nella scheda Dettagli della condivisione di file.

Per informazioni sul montaggio della condivisione di file, vedi Installare la condivisione di file SMB sul client.

Impostazioni di configurazione predefinite per le condivisioni di file SMB

Le seguenti impostazioni si applicano a tutte le nuove condivisioni di file SMB create utilizzando la configurazione predefinita. Dopo aver creato una condivisione di file, è possibile selezionarla dalla pagina Condivisioni di file nella console di AWS Storage Gateway per visualizzare i dettagli sulla sua configurazione.

> **Important**
>
> La configurazione predefinita della condivisione di file SMB fornisce il controllo completo dei file e le autorizzazioni di accesso al proprietario del bucket S3 mappato alla condivisione di file, anche se il bucket è di proprietà di un altro account Amazon Web Services. Per ulteriori informazioni sull'utilizzo della condivisione di file per accedere agli oggetti in un bucket di proprietà di un altro account, consulta Utilizzo di una condivisione di file per l'accesso tra account.

Impostazione	Valore predefinito	Note
Ubicazione Amazon S3	La condivisione di file si connette direttamente al bucket Amazon S3 e ha lo stesso nome del bucket. Il gateway utilizza questo bucket per archiviare e recuperare file.	Il nome non include un prefisso.
AWS PrivateLink per S3	La condivisione di file non si connette ad Amazon S3 tramite un endpoint di interfacc ia nel tuo cloud privato virtuale (VPC).	
Notifica di caricamento dei file	Disattivata	

Impostazione	Valore predefinito	Note
Classe di archiviazione per nuovi oggetti	Amazon S3 Standard	Ciò consente di archiviare i dati degli oggetti a cui si accede di frequente in modo ridondante in più zone di disponibilità separate geograficamente. Per ulteriori informazioni sulla classe di Amazon S3 Standard storage, consulta Classi di storage per oggetti a cui si accede di frequente nella Amazon Simple Storage Service User Guide.
Encryption (Crittografia)	Crittografia lato server con chiavi gestite S3 (SSE-S3)	Tutti gli oggetti Amazon S3 caricati, aggiornati o modificati da S3 File Gateway sono crittografati per impostazione predefinita con crittografia lato server utilizzando chiavi gestite di Amazon S3.

Impostazione	Valore predefinito	Note
Metadati degli oggetti	Indovina il tipo MIME	Ciò consente a Storage Gateway di indovinare il tipo MIME (Multipurpose Internet Mail Extension) per gli oggetti caricati in base alle estensioni di file. Questa opzione richiede che le liste di controllo degli accessi (ACLs) siano attivate per il bucket Amazon S3 associato alla condivisione di file. Se sono ACLs disattivata, la condivisione di file non può accedere al bucket Amazon S3 e rimane nello stato Non disponibile a tempo indetermi nato.
Enumerazione basata sull'accesso	Non attivata	I file e le cartelle presenti nella condivisione di file sono visibili a tutti gli utenti durante l'enumerazione delle directory . L'enumerazione basata sull'accesso è un sistema che filtra l'enumerazione di file e cartelle in una condivisione di file SMB in base all'acces so della condivisione liste di controllo (ACLs).

Impostazione	Valore predefinito	Note
Abilita i pagamenti del richiedente	Disattivata	Per ulteriori informazioni, consulta Bucket con pagamento a carico del richiedente.
Blocco opportunistico	Abilitato	Ciò consente alla condivisione di file di utilizzare il blocco opportunistico per ottimizzare la strategia di buffering dei file. Nella maggior parte dei casi, l'attivazione del blocco opportunistico migliora prestazioni, in particolare per quanto riguarda il contesto Windows menu.
Log di verifica	Disattivata	La registrazione a un Amazon CloudWatch gruppo è disattivata per impostazione predefinita.
Forza la sensibilità maiuscola	Disattivata	Ciò consente al client di controllare la distinzione tra maiuscole e minuscole.
Accesso al tuo bucket S3	Crea un nuovo ruolo IAM	L'opzione predefinita consente a File Gateway di creare un nuovo ruolo e accesso IAM politica per tuo conto.

Crea una condivisione di file SMB con una configurazione personalizzata

Utilizzare la procedura seguente per creare una condivisione di file Server Message Block (SMB) con una configurazione personalizzata. Per creare una condivisione di file SMB utilizzando le

impostazioni di configurazione predefinite, vedere Creare una condivisione di file SMB utilizzando la configurazione predefinita.

> **Important**
>
> L'utilizzo di S3 Versioning, Cross-Region Replication o dell'utilità Rsync durante il caricamento di dati da un File Gateway può avere implicazioni significative in termini di costi. Per ulteriori informazioni, consulta Evitare costi imprevisti durante il caricamento di dati da File Gateway.

Prerequisiti

Prima di creare la condivisione di file, procedi come segue:

- Configura le impostazioni di sicurezza SMB per il tuo File Gateway. Per istruzioni, consulta Impostazione di un livello di sicurezza per il gateway.
- Configura Microsoft Active Directory o l'accesso guest per l'autenticazione. Per istruzioni, consulta Utilizzo di Active Directory per autenticare gli utenti o Fornire l'accesso come ospite alla condivisione di file.
- Assicurati che le porte richieste siano aperte nel tuo gruppo di sicurezza. Per ulteriori informazioni, consulta Requisiti delle porte.

Per creare una condivisione di file SMB con impostazioni personalizzate

1. Apri la console AWS Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/ e scegli Condivisioni di file dal riquadro di navigazione a sinistra.
2. Scegliere Create file share (Crea condivisione file).
3. Scegli Personalizza configurazione. Per ora puoi ignorare gli altri campi di questa pagina. Nei passaggi successivi ti verrà richiesto di configurare le impostazioni del gateway, del protocollo e dello storage.
4. Per Gateway, scegli Amazon S3 File Gateway dall'elenco a discesa.
5. Per il gruppo di CloudWatch log, scegli una delle seguenti opzioni dall'elenco a discesa:
   - Per disattivare la registrazione per questa condivisione di file, scegli Disabilita registrazione.
   - Per creare automaticamente un nuovo gruppo di log per questa condivisione di file, scegliere Creato da Storage Gateway.

- Per inviare notifiche sullo stato e sulle risorse per questa condivisione di file a un gruppo di log esistente, scegli il gruppo desiderato dall'elenco.

Per ulteriori informazioni sui log di controllo, consulta Understanding S3 File Gateway audit logs.

6. (Facoltativo) In Tag - Facoltativo, scegli Aggiungi nuovo tag, quindi inserisci una chiave e un valore per la condivisione di file. Un tag è una coppia chiave-valore con distinzione tra maiuscole e minuscole che consente di classificare le risorse dello Storage Gateway. L'aggiunta di tag può semplificare il filtraggio e la ricerca della condivisione di file. Puoi ripetere questo passaggio per aggiungere fino a 50 tag.

   Al termine, scegli Avanti.

7. Per il bucket S3, esegui una delle seguenti operazioni per specificare dove archiviare e recuperare i file:

   - Per connettere la condivisione di file direttamente a un bucket S3 esistente nel tuo account Amazon Web Services, scegli il nome del bucket dall'elenco a discesa.
   - Per connettere la condivisione di file a un bucket S3 esistente di proprietà di un account Amazon Web Services diverso da quello che stai utilizzando per creare la condivisione di file, scegli Un bucket in un altro account dall'elenco a discesa, quindi inserisci il nome del bucket tra account.
   - Per connettere la condivisione di file a un nuovo bucket S3, scegli Crea un nuovo bucket S3, quindi scegli la regione in cui si trova l'endpoint Amazon S3 per il nuovo bucket e inserisci un nome di bucket S3 univoco. Al termine, scegli Crea bucket S3. Per ulteriori informazioni sulla creazione di nuovi bucket, vedi Come si crea un bucket S3? nella Guida per l'utente di Amazon S3.
   - Per connettere la condivisione di file a un bucket S3 utilizzando il nome di un punto di accesso, scegli il nome del punto di accesso Amazon S3 dall'elenco a discesa, quindi inserisci il nome del punto di accesso. Se devi creare un nuovo punto di accesso, puoi scegliere Crea un punto di accesso S3. Per ulteriori istruzioni, consulta Creazione di un punto di accesso nella Guida per l'utente di Amazon S3. Per ulteriori informazioni sui punti di accesso, consulta Gestire l'accesso ai dati con i punti di accesso Amazon S3 e Delegare il controllo degli accessi ai punti di accesso nella Amazon S3 User Guide.
   - Per connettere la condivisione di file a un bucket S3 utilizzando un alias del punto di accesso, scegli l'alias del punto di accesso Amazon S3 dall'elenco a discesa, quindi inserisci l'alias del punto di accesso. Se devi creare un nuovo punto di accesso, puoi scegliere Crea un punto di

accesso S3. Per ulteriori istruzioni, consulta Creazione di un punto di accesso nella Guida per l'utente di Amazon S3. Per ulteriori informazioni sugli alias dei punti di accesso, consulta Using a bucket alias for your access point nella Amazon S3 User Guide.

> **Note**
>
> Ogni condivisione di file può connettersi solo a un bucket S3, ma più condivisioni di file possono connettersi allo stesso bucket. Se connetti più di una condivisione di file allo stesso bucket, devi configurare ogni condivisione di file in modo che utilizzi un prefisso di bucket S3 univoco e non sovrapposto per evitare conflitti. read/write
> S3 File Gateway non supporta i bucket Amazon S3 con periodi . () nel nome del bucket. Assicurati che il nome del bucket sia conforme alle regole per la denominazione dei bucket in Amazon S3. Per ulteriori informazioni, consulta le Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

8. (Facoltativo) Per il prefisso del bucket S3, inserisci un prefisso per la condivisione di file da applicare agli oggetti che crea in Amazon S3. I prefissi sono un modo per organizzare i dati in S3, in modo simile alle directory nelle strutture di file tradizionali. Per ulteriori informazioni, consulta Organization objects using prefixes nella Amazon S3 User Guide.

> **Note**
>
> - Se connetti più di una condivisione di file allo stesso bucket, devi configurare ogni condivisione di file in modo che utilizzi un prefisso unico e non sovrapposto per evitare conflitti. read/write
> - Il prefisso deve terminare con una barra (/).
> - Dopo aver creato la condivisione di file, il prefisso non può essere modificato o eliminato.

9. Per Regione, scegli Regione AWS dove si trova l'endpoint S3 per il tuo bucket dall'elenco a discesa. Questo campo viene visualizzato solo quando specifichi un punto di accesso o un bucket in un altro account per il bucket S3.
10. Per Classe di archiviazione per nuovi oggetti, scegli una classe di archiviazione dall'elenco a discesa. Per ulteriori informazioni sulle classi di archiviazione, consulta Utilizzo delle classi di archiviazione con un File Gateway.

11. Per IAM Role, esegui una delle seguenti operazioni per configurare un ruolo IAM per la condivisione di file:

    - Per creare automaticamente un nuovo ruolo IAM con le autorizzazioni necessarie per il corretto funzionamento della condivisione di file, scegli Created by Storage Gateway dall'elenco a discesa.
    - Per utilizzare un ruolo IAM esistente, scegli il nome del ruolo dall'elenco a discesa.
    - Per creare un nuovo ruolo IAM, scegli Crea un ruolo. Per ulteriori istruzioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l' AWS Identity and Access Management utente.

    Per ulteriori informazioni su come i ruoli IAM controllano l'accesso tra la condivisione di file e il bucket S3, consulta Garantire l'accesso a un Amazon S3bucket.

12. Per Link privato, procedi come segue solo se devi configurare la condivisione di file con cui comunicare AWS utilizzando un endpoint privato in un Virtual Private Cloud (VPC). In caso contrario, puoi ignorare questo passaggio. Per ulteriori informazioni, consulta Cos'è? AWS PrivateLink nella AWS PrivateLink Guida.

    a. Seleziona Usa endpoint VPC.

    b. Per Identify VPC endpoint by, esegui una delle seguenti operazioni:

        - Seleziona ID endpoint VPC, quindi scegli l'endpoint che desideri utilizzare dall'elenco a discesa degli endpoint VPC.
        - Seleziona il nome DNS, quindi inserisci il nome DNS dell'endpoint che desideri utilizzare.

13. Per la crittografia, scegli il tipo di chiavi di crittografia da utilizzare per crittografare gli oggetti archiviati dal tuo File Gateway in Amazon S3:

    - Per utilizzare la crittografia lato server gestita con Amazon S3 (SSE-S3), scegli S3 Managed Keys (SSE-S3).

      Per ulteriori informazioni, consulta Usare la crittografia lato server con le chiavi gestite di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.
    - Per utilizzare la crittografia lato server gestita con AWS Key Management Service (SSE-KMS), scegli KMS-Managed Keys (SSE-KMS). Per la chiave KMS primaria, scegli una chiave KMS esistente o scegli Crea una nuova chiave AWS KMS per creare una nuova chiave KMS nella console del servizio di gestione delle chiavi (). AWS AWS KMS

Per ulteriori informazioni su AWS KMS, consulta Cos'è AWS il servizio di gestione delle chiavi? nella Guida per gli AWS Key Management Service sviluppatori.

- Per utilizzare la crittografia lato server a doppio livello gestita con AWS Key Management Service (DSSE-KMS), scegli la crittografia lato server a doppio livello con chiavi (DSSE-KMS). AWS Key Management Service Per la chiave KMS primaria, scegli una chiave KMS esistente o scegli Crea una nuova chiave AWS KMS per creare una nuova chiave KMS nella console Key Management Service (). AWS AWS KMS

  Per ulteriori informazioni su DSSE-KMS, consulta Uso della crittografia lato server a doppio livello con chiavi AWS KMS nella Guida per l'utente di Amazon Simple Storage Service.

  > **Note**
  >
  > Sono previsti costi aggiuntivi per l'utilizzo di DSSE-KMS e delle chiavi. AWS KMS Per ulteriori informazioni, consulta Prezzi di AWS KMS.
  > Per specificare una AWS KMS chiave con un alias non presente nell'elenco o per utilizzare una AWS KMS chiave di un AWS account diverso, è necessario utilizzare il. AWS Command Line Interface Le chiavi KMS asimmetriche non sono supportate. Per ulteriori informazioni, vedere Create SMBFile Share nello AWS Storage Gateway API Reference.

> **Important**
>
> Assicurati che la condivisione di file utilizzi lo stesso tipo di crittografia del bucket Amazon S3 in cui archivia i dati.

14. Per i tipi Guess MIME, selezionare il tipo MIME multimediale Guess per consentire a Storage Gateway di indovinare il tipo MIME (Multipurpose Internet Mail Extension) per gli oggetti caricati in base alle relative estensioni di file.
15. Per Nome di condivisione di file, inserisci un nome per la condivisione di file.

> **Note**
>
> Un nome di condivisione di file SMB valido non può contenere i seguenti caratteri: `[],#,;,<,>,:,",\,/,|, ? *+`, o caratteri di controllo ASCII. `1-31`

16. Per Eventi di caricamento, seleziona Registra un evento quando un file viene caricato correttamente dal gateway se desideri che il gateway registri gli eventi di CloudWatch registro quando carica correttamente i file su Amazon S3. Il ritardo di notifica controlla il ritardo tra l'operazione di scrittura del client più recente e la generazione della notifica di `ObjectUploaded` registro. Poiché i client possono eseguire molte piccole scritture su file in breve tempo, consigliamo di impostare questo parametro il più a lungo possibile per evitare di generare più notifiche per lo stesso file in rapida successione. Per ulteriori informazioni, consulta Ricevere una notifica di caricamento di file.

    > **Note**
    >
    > Questa impostazione non ha effetto sulla tempistica del caricamento dell'oggetto su S3, ma solo sulla tempistica della notifica.
    > Questa impostazione non ha lo scopo di specificare l'ora esatta in cui verrà inviata la notifica. In alcuni casi, il gateway potrebbe richiedere un tempo di ritardo superiore a quello specificato per generare e inviare notifiche.

    Al termine, scegli Avanti.

17. Per Protocollo di condivisione file, scegli SMB.
18. Per l'autenticazione utente, scegli il metodo di autenticazione che desideri utilizzare dall'elenco a discesa:

    - Per utilizzare Microsoft Active Directory aziendale o AWS Managed Microsoft AD per autenticare l'accesso degli utenti alla condivisione di file SMB, scegli Active Directory. Il gateway deve essere aggiunto a un dominio per utilizzare questo metodo. Per ulteriori informazioni, vedere Utilizzo di Active Directory per autenticare gli utenti.

      > **Note**
      >
      > Per AWS Managed Microsoft AD utilizzarla con un EC2 gateway Amazon, devi creare l' EC2 istanza Amazon nello stesso VPC di AWS Managed Microsoft AD, aggiungere il gruppo di `_workspaceMembers` sicurezza all' EC2istanza Amazon e unirti al dominio AD utilizzando le credenziali di amministratore di. AWS Managed Microsoft AD
      > Per ulteriori informazioni in merito AWS Managed Microsoft AD, consulta la Guida all'AWS Directory Service amministrazione.

Per ulteriori informazioni su Amazon EC2, consulta la documentazione di Amazon Elastic Compute Cloud.

Se lo stato di accesso indica che il gateway è già aggiunto a un dominio Active Directory, procedi al passaggio successivo. In caso contrario, eseguire le seguenti operazioni:

1. Scegli Configura.
2. Per Dominio, inserisci il nome del dominio Active Directory a cui desideri aggiungere il gateway.
3. Inserisci il nome utente e la password che il gateway utilizzerà per accedere al dominio.
4. (Facoltativo) Per Unità organizzativa (OU), immettere l'unità organizzativa designata utilizzata da Active Directory per i nuovi oggetti del computer.
5. (Facoltativo) Per i controller di dominio (DC), immettete il nome del controller di dominio tramite il quale il gateway si connetterà ad Active Directory. Puoi lasciare vuoto questo campo per consentire al DNS di selezionare automaticamente un DC.
6. Scegli Iscriviti ad Active Directory.

> **Note**
>
> L'aggiunta a un dominio crea un account Active Directory nel contenitore predefinito (che non è un'unità organizzativa), utilizzando l'ID Gateway del gateway come nome dell'account (ad esempio, SGW-1234ADE). Non è possibile personalizzare il nome di questo account.
> Se l'ambiente Active Directory richiede la preconfigurazione degli account per facilitare il processo di aggiunta al dominio, è necessario creare questo account in anticipo.
> Se l'ambiente Active Directory dispone di un'unità organizzativa designata per i nuovi oggetti del computer, è necessario specificare tale unità organizzativa al momento dell'accesso al dominio.

- Per concedere l'accesso protetto da password a chiunque fornisca la password guest configurata, scegli Accesso ospite. Non è necessario che File Gateway faccia parte di un dominio Microsoft Active Directory per utilizzare questo metodo. Scegli Configura per specificare la tua password Guest, quindi scegli Salva.

19. Per l'accesso utente, esegui una delle seguenti operazioni per specificare quali client SMB possono accedere alla condivisione di file:

- Per concedere l'accesso a tutti gli utenti che si autenticano correttamente tramite Active Directory, seleziona Tutti gli utenti autenticati da Active Directory.
- Per consentire o negare l'accesso a utenti o gruppi specifici, scegli Utenti o gruppi specifici con autenticazione AD, quindi procedi come segue:
  - Per Utenti e gruppi consentiti, scegli Aggiungi utente consentito o Aggiungi gruppo consentito e inserisci un utente o un gruppo di Active Directory a cui desideri consentire l'accesso alla condivisione di file. Ripeti questa procedura per consentire il numero di utenti e gruppi necessario
  - Per Utenti e gruppi negati, scegli Aggiungi utente negato o Aggiungi gruppo negato e inserisci un utente o un gruppo di Active Directory a cui desideri negare l'accesso alla condivisione di file. Ripeti questa procedura per negare il numero di utenti e gruppi necessario.

> **Note**
>
> La sezione Accesso alla condivisione di file di utenti e gruppi viene visualizzata solo se l'autenticazione utente è impostata su Active Directory.
> Quando specificate utenti o gruppi, non includete il dominio. Il nome di dominio è implicito nell'appartenenza del gateway alla specifica Active Directory a cui è unito.

20. (Facoltativo) Per gli utenti amministratori, immettete un elenco separato da virgole di utenti e gruppi di Active Directory. Gli utenti amministratori ricevono i privilegi per aggiornare gli elenchi di controllo degli accessi (ACLs) su tutti i file e le cartelle nella condivisione di file. I gruppi devono avere il prefisso del `@` carattere, ad esempio. `@group1`
21. Per Tipo di accesso, selezionare una delle seguenti opzioni:
    - Per consentire ai client di leggere e scrivere file sulla condivisione di file, seleziona Lettura/scrittura.
    - Per consentire ai client di leggere i file ma non di scrivere nella condivisione di file, seleziona Sola lettura.

> **Note**
>
> Per le condivisioni di file montate su un client Microsoft Windows, se si sceglie Sola lettura, è possibile che venga visualizzato un messaggio relativo a un errore imprevisto che impedisce di creare la cartella. Ignorare questo messaggio.

22. Per il controllo dell'accesso a file e directory, seleziona una delle seguenti opzioni:

    - Per impostare autorizzazioni dettagliate su file e cartelle nella condivisione di file SMB, seleziona Windows Access Control List. Per ulteriori informazioni, vedere Utilizzo di Microsoft Windows ACLs per controllare l'accesso a una condivisione di file SMB.
    - Per utilizzare le autorizzazioni POSIX per controllare l'accesso a file e directory archiviati tramite la condivisione di file SMB, scegli le autorizzazioni POSIX.

23. Per l'enumerazione basata su Access, effettuate una delle seguenti operazioni:

    - Per rendere visibili i file e le cartelle della condivisione solo agli utenti con accesso in lettura, seleziona Nascondi file e directory per cui l'utente non dispone dell'autorizzazione.
    - Per rendere visibili i file e le cartelle della condivisione a tutti gli utenti durante l'enumerazione delle directory, non selezionare la casella di controllo.

> **Note**
>
> L'enumerazione basata sull'accesso è un sistema che filtra l'enumerazione di file e cartelle in una condivisione di file SMB in base agli elenchi di controllo di accesso della condivisione (). ACLs

24. Per le opzioni di accesso ai file, selezionare una delle seguenti opzioni:

    - Per ottimizzare la strategia di buffering dei file della condivisione di file utilizzando il blocco opportunistico, seleziona Blocco opportunistico. Nella maggior parte dei casi, l'attivazione del blocco opportunistico migliora le prestazioni, in particolare per quanto riguarda i menu contestuali di Windows.
    - Per consentire al gateway, anziché al client SMB, di controllare la distinzione tra maiuscole e minuscole per nome file, seleziona Forza la distinzione tra maiuscole e minuscole.
    - Per disattivare entrambe le impostazioni, seleziona Nessuna delle due.

> **Note**
>
> Per evitare conflitti di accesso ai file, queste impostazioni si escludono a vicenda e non possono essere attivate contemporaneamente.

25. (Facoltativo) Per l'aggiornamento automatico della cache da S3, scegli Imposta intervallo di aggiornamento della cache, quindi imposta il tempo in minuti o giorni per aggiornare la cache della condivisione di file utilizzando Time To Live (TTL). TTL è il periodo di tempo trascorso dall'ultimo aggiornamento. Trascorso l'intervallo TTL, l'accesso a una directory fa sì che File Gateway aggiorni i contenuti di quella directory dal bucket Amazon S3.

    > **Note**
    >
    > L'impostazione di questo valore in un periodo inferiore a 30 minuti può influire negativamente sulle prestazioni del gateway in situazioni in cui viene spesso creato o eliminato un numero elevato di oggetti Amazon S3.

26. Per la proprietà e le autorizzazioni dei file, seleziona Assegna al proprietario del bucket S3 la piena proprietà dei file creati dal gateway, incluse le autorizzazioni di lettura, scrittura, modifica ed eliminazione, se desideri che l' AWS account proprietario del bucket S3 abbia il pieno controllo di tutti gli oggetti scritti nel bucket dalla tua condivisione di file.

    Al termine, scegli Avanti.

27. Rivedi la configurazione della condivisione dei file. Scegli Modifica per modificare le impostazioni di qualsiasi sezione che desideri modificare. Al termine, scegli Create (Crea).

Dopo aver creato la condivisione di file SMB, è possibile visualizzarne le impostazioni di configurazione nella console AWS Storage Gateway nella scheda Dettagli della condivisione di file. Per istruzioni su come montare la condivisione di file, vedi Installare la condivisione di file SMB sul client.

Montaggio e utilizzo della condivisione di file

Gli argomenti di questa sezione forniscono istruzioni su come montare la condivisione di file sul client, utilizzare la condivisione di file, testare il File Gateway e ripulire le risorse che non sono più necessarie, come i gateway, le istanze Amazon o EC2 le istanze locali VMs che potresti creare a scopo di test. Per ulteriori informazioni sui client Network File System (NFS) e Service Message Block (SMB) supportati, consulta. Client NFS e SMB supportati per File Gateway

> **Note**
>
> Fornisce Console di gestione AWS anche alcuni comandi di esempio che è possibile utilizzare per montare la condivisione di file.

Argomenti

- Installa la condivisione di file NFS sul tuo client- Scopri come montare la tua condivisione di file NFS su un'unità del tuo client e mapparla sul tuo bucket Amazon S3.
- Installa la tua condivisione di file SMB sul tuo client- Scopri come montare la tua condivisione di file SMB e mapparla su un'unità accessibile al tuo cliente.
- Utilizzo di condivisioni di file su bucket con oggetti preesistenti- Scopri come esportare una condivisione di file su un bucket Amazon S3 con oggetti creati all'esterno del File Gateway utilizzando NFS o SMB.
- Metti alla prova il tuo S3 File Gateway- Scopri come testare il tuo gateway copiando file e cartelle sull'unità mappata e verificando che compaiano automaticamente nel tuo bucket Amazon S3.

Installa la condivisione di file NFS sul tuo client

Utilizza la seguente procedura per montare la condivisione di file NFS su un'unità del client e mapparla al bucket Amazon S3.

Per montare una condivisione di file e mapparla su un bucket Amazon S3

1. Se si sta utilizzando un client di Microsoft Windows, è consigliabile creare una condivisione file SMB e accedervi usando un client SMB già installato sul client di Windows. Se si utilizza NFS, attivare Servizi per NFS in Windows.

2. Montaggio della condivisione file NFS:

   - Per i client Linux, digitare il comando seguente al prompt dei comandi.

     ```
     sudo mount -t nfs -o nolock,hard [GatewayVMIPAddress]:/[FileShareName]
     [ClientMountPath]
     ```

   - Per i client Windows, digita il seguente comando al prompt dei comandi (cmd.exe).

     ```
     mount -o nolock -o mtype=hard [GatewayVMIPAddress]:/[FileShareName]
     [WindowsDriveLetter]
     ```

Ad esempio, supponiamo che su un client Windows l'indirizzo IP della macchina virtuale sia 123.123.1.2 e che il nome della condivisione di file sia. `test-fileshare` voglia mappare la condivisione all'unità T. In questo caso, il comando appare come segue.

```
mount -o nolock -o mtype=hard 123.123.1.2:/test-fileshare T:
```

> **Note**
>
> Durante il montaggio della condivisione file, tieni presente quanto segue:
>
> - Per impostazione predefinita, Windows utilizza un soft mount per le condivisioni NFS. I soft mount si interrompono più facilmente quando si verificano problemi di connessione. Consigliamo di utilizzare un supporto rigido per carichi di lavoro critici, poiché i supporti rigidi sono più sicuri e preservano meglio i dati. Per utilizzare un supporto rigido, assicurati che il comando utilizzi lo `-o mtype=hard` switch.
> - S3 File Gateway non supporta il blocco dei file NFS. Utilizzate sempre l'`-o nolock`opzione per disattivare il blocco dei file quando montate le condivisioni di file NFS.
> - Potresti avere un caso in cui una cartella e un oggetto esistono in un bucket Amazon S3 e hanno lo stesso nome. In questo caso, se il nome dell'oggetto non contiene una barra finale, in un File Gateway è visibile solo la cartella. Ad esempio, se un bucket contiene un oggetto denominato `test` or `test/` e una cartella denominata`test/test1`, `test/test1` sono visibili solo `test/` e solo in un File Gateway.
> - Potrebbe essere necessario rimontare la condivisione file dopo il riavvio del client.
> - Se si utilizzano client Windows, verificare le opzioni `mount` dopo il montaggio eseguendo il comando `mount` senza opzioni. La risposta deve confermare che la

condivisione file è stata montata utilizzando le ultime opzioni fornite. Inoltre, deve confermare che non si utilizzano voci precedentemente memorizzate nella cache, che richiedono almeno 60 secondi per essere cancellate.

Fase successiva

Metti alla prova il tuo S3 File Gateway

Installa la tua condivisione di file SMB sul tuo client

Utilizza le seguenti procedure per montare la condivisione di file SMB e mapparla su un'unità accessibile al tuo client. La sezione File Gateway della console mostra i comandi di montaggio supportati che è possibile utilizzare per i client SMB. Di seguito puoi trovare ulteriori opzioni disponibili.

Esistono più metodi per montare una condivisione file SMB, tra cui i seguenti:

- Command Prompt (`cmdkey`and`net use`): utilizza il prompt dei comandi per montare la condivisione di file. Archivia le tue credenziali con`cmdkey`, quindi monta l'unità `net use` e includi gli `/savecred` switch `/persistent:yes` e se desideri che la connessione persista anche dopo i riavvii del sistema. I comandi specifici utilizzati saranno diversi a seconda che si desideri montare l'unità per l'accesso a Microsoft Active Directory (AD) o per l'accesso come utente ospite. Di seguito sono riportati alcuni esempi.
- File Explorer (Map Network Drive): utilizza Windows File Explorer per montare la condivisione di file. Configura le impostazioni per specificare se desideri che la connessione persista anche dopo i riavvii del sistema e richiedi le credenziali di rete.
- PowerShell script: crea uno PowerShell script personalizzato per montare la condivisione di file. A seconda dei parametri specificati nello script, la connessione può essere persistente anche dopo i riavvii del sistema e la condivisione può essere visibile o invisibile al sistema operativo durante il montaggio.

> **Note**
>
> Se sei un utente Microsoft AD, consulta l'amministratore per verificare di avere accesso alla condivisione file SMB prima di montare la condivisione file sul sistema locale.

Se sei un utente ospite, assicurati di disporre della password dell'utente ospite prima di provare a montare la condivisione di file.

Per montare la condivisione di file SMB per gli utenti autorizzati di Microsoft AD utilizzando il prompt dei comandi:

1. Assicurati che l'utente Microsoft AD disponga delle autorizzazioni necessarie per la condivisione di file SMB prima di montare la condivisione di file sul sistema dell'utente.
2. Immettete quanto segue al prompt dei comandi per montare la condivisione di file:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes
   ```

Per montare la condivisione di file SMB con una combinazione di credenziali di accesso specifica utilizzando il prompt dei comandi:

1. Assicurati che l'utente abbia accesso alla condivisione di file SMB prima di montare la condivisione di file sul sistema.
2. Immettete quanto segue al prompt dei comandi per salvare le credenziali utente in Windows Credential Manager:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. Immettere quanto segue al prompt dei comandi per montare la condivisione di file:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes /savecred
   ```

Per montare la condivisione di file SMB per gli utenti ospiti utilizzando il prompt dei comandi:

1. Assicurati di avere la password dell'utente ospite prima di montare la condivisione di file.
2. Digitate quanto segue al prompt dei comandi per salvare le credenziali guest in Windows Credential Manager:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```
3. Digitare quanto segue al prompt dei comandi.

```
net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$Gateway
ID\smbguest /persistent:yes /savecred
```

> **Note**
>
> Durante il montaggio della condivisione file, tieni presente quanto segue:
>
> - Potresti avere un caso in cui una cartella e un oggetto esistono in un bucket Amazon S3 e hanno lo stesso nome. In questo caso, se il nome dell'oggetto non contiene una barra finale, in un File Gateway è visibile solo la cartella. Ad esempio, se un bucket contiene un oggetto denominato `test` or `test/` e una cartella denominata`test/test1`, `test/test1` sono visibili solo `test/` e solo in un File Gateway.
> - A meno che non si configuri la connessione di condivisione dei file per salvare le credenziali utente e mantenerla anche dopo i riavvii del sistema, potrebbe essere necessario rimontare la condivisione di file ogni volta che si riavvia il sistema client.

Montaggio di una condivisione file SMB con Esplora file di Windows

1. Premere il tasto Windows e digitare **File Explorer** nella casella Cerca in Windows per eseguire la ricerca o premere **Win+E**.
2. Nel pannello di navigazione, scegli Questo PC. Quindi, nella scheda Computer, scegli Map Network Drive.
3. Nella finestra di dialogo Connetti unità di rete, scegliere una lettera di unità per Unità.
4. Per Cartella, digitare ***[File Gateway IP]**[SMB File Share Name]***, oppure scegliere Sfoglia per selezionare la condivisione file SMB dalla finestra di dialogo.
5. (Facoltativo) Selezionare Riconnetti all'accesso se si desidera che il punto di montaggio persista anche dopo un riavvio.
6. (Facoltativo) Selezionare Connetti con credenziali diverse se si desidera che l'utente immetta la password dell'account guest o di accesso a Microsoft AD.
7. Scegliere Fine per completare il punto di montaggio.

> **Note**
>
> Tutti i file o le cartelle che iniziano con un punto (`.`) verranno contrassegnati come nascosti in Windows. Per rendere visibili questi file e cartelle, è necessario selezionare la casella di controllo Elementi nascosti nella scheda Visualizza in Esplora file di Windows.

Dalla console di gestione Storage Gateway puoi modificare le impostazioni della condivisione file, gli utenti e i gruppi a cui è consentito o negato l'accesso, nonché la password per l'accesso non autenticato (guest). Inoltre, hai la possibilità di aggiornare i dati nella cache della condivisione file ed eliminare una condivisione file dalla console.

Come modificare le proprietà della condivisione file SMB

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione, selezionare File Shares (Condivisioni di file).
3. Nella pagina File Share (Condivisione file), selezionare la casella di controllo della condivisione file SMB da modificare.
4. Tra le Operazioni, scegliere quella desiderata:

   - Selezionare Edit file share settings (Modifica le impostazioni della condivisione file) per modificare l'accesso alla condivisione.
   - Scegli Modifica allowed/denied utenti per aggiungere o eliminare utenti e gruppi, quindi digita gli utenti e i gruppi consentiti e negati nelle caselle Utenti consentiti, Utenti negati, Gruppi consentiti e Gruppi negati. Utilizzare i pulsanti Add Entry (Aggiungi voce) per concedere nuovi diritti di accesso e la (X) per rimuovere un accesso.

     > **Note**
     >
     > I gruppi devono avere il prefisso del `@` carattere. I formati accettabili includono: `DOMAIN\User1user1`,`@group1`, e`@DOMAIN\group1`.

5. Al termine, selezionare Save (Salva).

   Quando si immettono utenti e gruppi consentiti, si crea un elenco di utenti consentiti. Senza un elenco di file consentiti, tutti gli utenti autenticati di Microsoft AD possono accedere alla condivisione di file SMB. Tutti gli utenti e i gruppi contrassegnati come negati vengono aggiunti a un elenco di utenti non autorizzati e non possono accedere alla condivisione di file SMB. Nei casi

in cui un utente o un gruppo è presente sia nell'elenco degli utenti non autorizzati che nell'elenco degli utenti consentiti, l'elenco degli utenti non autorizzati ha la precedenza.

È possibile attivare Access Control Lists (ACLs) sulla condivisione di file SMB. Per informazioni su come attivarla ACLs, consultaUtilizzo di Windows ACLs per limitare l'accesso alla condivisione di file SMB.

Fase successiva

Metti alla prova il tuo S3 File Gateway

Utilizzo di condivisioni di file su bucket con oggetti preesistenti

Puoi esportare una condivisione di file su un bucket Amazon S3 con oggetti creati all'esterno del File Gateway utilizzando NFS o SMB. Quando i client di file system vi accedono, gli oggetti del bucket creati al di fuori del gateway vengono visualizzati come file, sia nel file system NFS sia in quello SMB. Nella condivisione file vengono adoperati l'accesso e le autorizzazioni POSIX (Portable Operating System Interface) standard. Quando riscrivi i file in un bucket Amazon S3, i file assumono le proprietà e i diritti di accesso che concedi loro.

È possibile caricare oggetti in un bucket S3 in qualsiasi momento. Affinché la condivisione file mostri gli oggetti appena aggiunti come file, occorre innanzitutto aggiornare il bucket S3. Per ulteriori informazioni, consulta the section called “Aggiornamento della cache degli oggetti del bucket Amazon S3”.

> **Note**
>
> Non è consigliabile avere più writer per un bucket Amazon S3. In tal caso, assicurati di leggere la sezione «Posso avere più writer nel mio bucket Amazon S3?» nelle domande frequenti su Storage Gateway.

Per assegnare le impostazioni predefinite dei metadati agli oggetti con accesso mediante NFS, consulta Modificare le impostazioni predefinite dei metadati in Gestione del tuo Amazon S3 File Gateway.

Per le PMI, puoi esportare una condivisione utilizzando Microsoft AD o l'accesso guest per un bucket Amazon S3 con oggetti preesistenti. Gli oggetti esportati tramite una condivisione file SMB ereditano

la proprietà e le autorizzazioni POSIX dalla directory principale immediatamente superiore. Gli oggetti nella cartella principale ereditano le liste di controllo accessi (ACL) principali. Per l'ACL principale, il proprietario è `smbguest`, le autorizzazioni per i file sono 666 e, infine, le directory sono 777. Quanto scritto si applica a tutte le forme di accesso autenticato (Microsoft AD e guest).

Metti alla prova il tuo S3 File Gateway

Utilizza la seguente procedura per testare il gateway copiando file e cartelle sull'unità mappata e verificando che compaiano automaticamente nel tuo bucket Amazon S3.

Per caricare file dal tuo client Windows su Amazon S3

1. Dal client Windows, accedere all'unità sulla quale è stata montata la condivisione file. Il nome dell'unità è preceduto da quello del bucket S3.
2. Copiare i file o una cartella sull'unità.
3. Nella console di gestione Amazon S3, accedi al bucket mappato. Dovresti vedere i file e le cartelle che hai copiato nel bucket Amazon S3 che hai specificato.

   È possibile visualizzare la condivisione di file creata nella scheda Condivisioni di file nella console di gestione AWS di Storage Gateway.

Il client NFS o SMB può scrivere, leggere, eliminare, rinominare e troncare i file.

> **Note**
>
> I File Gateway non supportano la creazione di link fissi o simbolici su una condivisione di file.

Tieni a mente questi punti su come i File Gateway funzionano con S3:

- Le letture vengono eseguite da una cache read-through, di lettura passante. In altre parole, se non sono disponibili, i dati vengono recuperati da S3 e aggiunti alla cache.
- Le scritture vengono inviate a S3 tramite caricamenti in più parti ottimizzati con l'ausilio di una cache write-back, di riscrittura.
- Le operazioni di lettura e scrittura sono ottimizzate in modo tale che solo le parti richieste o modificate vengano trasferite sulla rete.
- Le eliminazioni rimuovono gli oggetti da S3.

- Le directory vengono gestite come oggetti cartella in S3, utilizzando la stessa sintassi della console Amazon S3. Le directory vuote possono essere rinominate.
- Le prestazioni operative del file system con l'algoritmo ricorsivo (ad esempio, `ls -l`) dipendono dal numero di oggetti nel bucket.

Gestione del tuo Amazon S3 File Gateway

Gli argomenti di questa sezione forniscono informazioni su come gestire le risorse di Amazon S3 File Gateway. La gestione del gateway include la concessione delle autorizzazioni per il gateway per accedere alle condivisioni di file e ai bucket Amazon S3, la modifica di informazioni e impostazioni per gateway e condivisioni di file, l'eliminazione di condivisioni di file, l'aggiornamento degli oggetti memorizzati nella cache e la comprensione degli indicatori di stato operativo per gateway e condivisioni di file.

Argomenti

- Modifica le informazioni di base sul gateway- Scopri come utilizzare la console Storage Gateway per modificare le informazioni di base per un gateway esistente, inclusi il nome del gateway, il fuso orario e il gruppo di CloudWatch log.
- Concessione dell'accesso e delle autorizzazioni- Scopri come utilizzare i ruoli IAM per fornire al tuo gateway le autorizzazioni di accesso per i bucket Amazon S3 e gli endpoint Amazon VPC, prevenire determinati problemi di sicurezza e connettere le condivisioni di file ai bucket tra account. AWS
- Eliminare una condivisione di file- Scopri come eliminare una condivisione di file utilizzando la console Storage Gateway.
- Modifica delle impostazioni SMB del gateway- Scopri come modificare le impostazioni SMB a livello di gateway che controllano la strategia di sicurezza, l'autenticazione Active Directory, l'accesso degli ospiti, le autorizzazioni dei gruppi locali e la visibilità della condivisione di file per le condivisioni di file SMB su un gateway.
- Modifica le impostazioni di condivisione di file SMB- Scopri come modificare le impostazioni per configurare nome, registrazione, aggiornamento della cache, classe di archiviazione, esportazione di file e altro per una condivisione di file SMB.
- Limita l'accesso alla condivisione di file SMB- Scopri come aggiungere utenti o gruppi consentiti o negati per limitare l'accesso alla condivisione di file SMB.
- Modifica le impostazioni di condivisione dei file NFS- Scopri come modificare le impostazioni per configurare nome, registrazione, aggiornamento della cache, classe di archiviazione, esportazione di file e altro per una condivisione di file NFS.
- Modifica le impostazioni predefinite dei metadati per la condivisione di file NFS- Scopri come modificare i valori dei metadati predefiniti che includono le autorizzazioni Unix per file e cartelle nelle condivisioni di file NFS.

- Limita l'accesso alla condivisione di file NFS- Scopri come limitare l'accesso ai client da indirizzi IP o intervalli IP specifici per la condivisione di file NFS.
- Aggiornamento della cache degli oggetti del bucket Amazon S3- Scopri come aggiornare la cache degli oggetti del bucket S3 per una condivisione di file e configurare una pianificazione per l'aggiornamento automatico della cache.
- Utilizzo del blocco oggetti S3- Scopri come funziona Amazon S3 File Gateway con la funzionalità S3 Object Lock.
- Stato della condivisione dei file- Scopri come visualizzare e interpretare lo stato della condivisione dei file.
- Stato del gateway- Scopri come visualizzare e interpretare lo stato del gateway.
- Gestione della larghezza di banda per Amazon S3 File Gateway- Scopri come limitare la velocità di upload dal gateway per AWS controllare la quantità di larghezza di banda di rete utilizzata dal gateway.

Modifica le informazioni di base per un S3 File Gateway

È possibile utilizzare la console Storage Gateway per modificare le informazioni di base per un gateway esistente, tra cui il nome del gateway, il fuso orario e il gruppo di CloudWatch log.

Per modificare le informazioni di base per un gateway esistente

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le informazioni di base.
3. Dal menu a discesa Operazioni, scegli Modifica le informazioni sul gateway.
4. Per Gateway name (Nome gateway), inserire un nome per il gateway. È possibile cercare questo nome per trovare il gateway nelle pagine di elenco della console Storage Gateway.

> **Note**
>
> I nomi dei gateway devono contenere tra 2 e 255 caratteri e non possono includere una barra (\o/).
> La modifica del nome di un gateway disconnetterà tutti gli CloudWatch allarmi impostati per monitorare il gateway. Per ricollegare gli allarmi, aggiorna il file GatewayNameper ogni allarme nella console. CloudWatch

5. Per il Fuso orario del gateway, scegli il fuso orario locale per la parte del mondo in cui desideri implementare il gateway.
6. Per Scegli come configurare un gruppo di log, scegli come configurare Amazon CloudWatch Logs per monitorare lo stato del tuo gateway. Scegliere tra le seguenti opzioni:
   - Crea un nuovo gruppo di log: configura un nuovo gruppo di log per monitorare il tuo gateway.
   - Usa un gruppo di log esistente: scegli un gruppo di log esistente dall'elenco a discesa corrispondente.
   - Disattiva la registrazione: non utilizzare Amazon CloudWatch Logs per monitorare il gateway.
7. Quando hai finito di modificare le impostazioni che desideri modificare, scegli Salva modifiche.

Concessione dell'accesso e delle autorizzazioni per le condivisioni di file e i bucket

Dopo l'attivazione e l'esecuzione di S3 File Gateway, puoi aggiungere ulteriori condivisioni di file e concedere l'accesso ai bucket Amazon S3, inclusi i bucket Account AWS diversi dai gateway e dalle condivisioni di file. Le seguenti sezioni descrivono come utilizzare i ruoli IAM per fornire al gateway le autorizzazioni di accesso per i bucket Amazon S3 e gli endpoint VPC, prevenire determinati problemi di sicurezza e connettere le condivisioni di file ai bucket. Account AWS

Per informazioni su come creare una nuova condivisione di file, consulta. Creazione di una condivisione file

Questa sezione contiene i seguenti argomenti, che forniscono informazioni aggiuntive su come concedere l'accesso e le autorizzazioni per le condivisioni di file e i bucket Amazon S3:

Argomenti

- Concessione dell'accesso a un bucket Amazon S3- Scopri come concedere l'accesso al tuo File Gateway per caricare file nel tuo bucket Amazon S3 ed eseguire azioni su qualsiasi punto di accesso o endpoint Amazon Virtual Private Cloud (Amazon VPC) che utilizza per connettersi al bucket.
- Prevenzione del problema "confused deputy" tra servizi- Scopri come prevenire un problema di sicurezza comune in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità con più privilegi a eseguire l'azione.

- Utilizzo di una condivisione di file per l'accesso a più account- Scopri come concedere l'accesso a un account Amazon Web Services e agli utenti di quell'account accedere a risorse che appartengono a un altro account Amazon Web Services.

Concessione dell'accesso a un bucket Amazon S3

Quando crei una condivisione di file, il tuo File Gateway richiede l'accesso per caricare i file nel tuo bucket Amazon S3 e per eseguire azioni su qualsiasi punto di accesso o endpoint del cloud privato virtuale (VPC) che utilizza per connettersi al bucket. Per concedere questo accesso, il File Gateway assume un ruolo AWS Identity and Access Management (IAM) associato a una policy IAM che concede tale accesso.

Il ruolo richiede questa policy IAM e una relazione di trust Security Token Service (STS) per la policy. La policy determina quali operazioni può eseguire il ruolo. Inoltre, il bucket S3 e tutti gli access point o endpoint VPC associati devono disporre di una policy di accesso che consenta al ruolo IAM di accedervi.

Puoi creare tu stesso il ruolo e la policy di accesso oppure il File Gateway può crearli per te. Se il tuo File Gateway crea la policy per te, la policy contiene un elenco di azioni S3. Per informazioni su ruoli e autorizzazioni, consulta Creating a role to delegate permissions to a un utente Servizio AWS nella IAM User Guide.

L'esempio seguente è una policy di fiducia che consente a File Gateway di assumere un ruolo IAM.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

> **Important**
>
> Storage Gateway può assumere ruoli di servizio esistenti che vengono passati utilizzando l'azione delle `iam:PassRole` policy, ma non supporta le policy IAM che utilizzano la chiave di `iam:PassedToService` contesto per limitare l'azione a servizi specifici.
> Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS Identity and Access Management :
>
> - IAM: passa un ruolo IAM a un AWS servizio specifico
> - Concessione a un utente delle autorizzazioni per trasferire un ruolo a un servizio AWS
> - Chiavi disponibili per IAM

Se non desideri che File Gateway crei una policy per tuo conto, puoi creare una policy personalizzata e allegarla alla condivisione di file. Per ulteriori informazioni su come effettuare tale operazione, consulta Creazione di una condivisione file.

La seguente policy di esempio consente a File Gateway di eseguire tutte le azioni di Amazon S3 elencate nella policy. La prima parte dell'istruzione permette l'esecuzione nel bucket S3 denominato `amzn-s3-demo-bucket` di tutte le operazioni elencate. La seconda parte permette le operazioni elencate su tutti gli oggetti in `amzn-s3-demo-bucket`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Effect": "Allow"
        }
    ]
}
```

La seguente policy di esempio è simile alla precedente, ma consente a File Gateway di eseguire le azioni necessarie per accedere a un bucket tramite un punto di accesso.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
```

```
        }
    ]
}
```

> **Note**
>
> Se devi connettere la tua condivisione di file a un bucket S3 tramite un endpoint VPC, consulta le politiche degli endpoint per Amazon S3 nella Guida per l'utente.AWS PrivateLink

> **Note**
>
> Per i bucket crittografati, il fileshare deve utilizzare la chiave nell'account bucket S3 di destinazione.

> **Note**
>
> Se il tuo File Gateway utilizza SSE-KMS o DSSE-KMS per la crittografia, assicurati che il ruolo IAM associato alla condivisione di file includa le autorizzazioni KMS:Encrypt, KMS:Decrypt, kms: *, kms: e kms:. ReEncrypt GenerateDataKey DescribeKey Per ulteriori informazioni, consulta Using Identity-Based Policies (IAM Policies) for Storage Gateway.

Prevenzione del problema "confused deputy" tra servizi

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse dell'account.

Si consiglia di utilizzare `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni che

Gateway di archiviazione AWS forniscono un altro servizio alla risorsa. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account nella stessa istruzione di policy.

Il valore di `aws:SourceArn` deve essere l'ARN dello Storage Gateway a cui è associata la condivisione di file.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`.

L'esempio seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition in Storage Gateway per evitare il confuso problema del vice.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Sid": "ConfusedDeputyPreventionExamplePolicy",
       "Effect": "Allow",
       "Principal": {
         "Service": "storagegateway.amazonaws.com"
       },
       "Action": "sts:AssumeRole",
       "Condition": {
         "StringEquals": {
           "aws:SourceAccount": "444455556666"
         },
         "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-
east-1:444455556666:gateway/sgw-123456DA"
        }
      }
    }
  ]
}
```

Utilizzo di una condivisione di file per l'accesso a più account

L'accesso tra account avviene quando un account Amazon Web Services e gli utenti di tale account ottengono l'accesso a risorse che appartengono a un altro account Amazon Web Services. Con File Gateways, puoi utilizzare una condivisione di file in un account Amazon Web Services per accedere agli oggetti in un bucket Amazon S3 che appartiene a un altro account Amazon Web Services.

Utilizzare una condivisione di file di proprietà di un account Amazon Web Services per accedere a un bucket S3 in un altro account Amazon Web Services

1. Assicurati che il proprietario del bucket S3 abbia concesso al tuo account Amazon Web Services l'accesso al bucket S3 a cui devi accedere e agli oggetti in quel bucket. Per informazioni su come concedere questo accesso, consulta l'Esempio 2: Il proprietario del bucket concede le autorizzazioni per i bucket tra account nella Guida per l'utente di Amazon Simple Storage Service. Per un elenco delle autorizzazioni richieste, consulta Concessione dell'accesso a un bucket Amazon S3.
2. Accertare che il ruolo IAM utilizzato dalla condivisione file per accedere al bucket S3 includa le autorizzazioni per operazioni quali `s3:GetObjectAcl` e `s3:PutObjectAcl`. Inoltre, verificare che il ruolo IAM includa una policy di attendibilità che consente all'account di assumere quel ruolo IAM. Per un esempio di policy di attendibilità, consulta Concessione dell'accesso a un bucket Amazon S3.

   Se la condivisione file utilizza un ruolo esistente per accedere al bucket S3, è necessario includere le autorizzazioni per le operazioni `s3:GetObjectAcl` e `s3:PutObjectAcl`. Il ruolo richiede inoltre una policy di attendibilità che consente all'account di assumere questo ruolo. Per un esempio di policy di attendibilità, consulta Concessione dell'accesso a un bucket Amazon S3.
3. Scegli i file Gateway accessibili al proprietario del bucket S3 quando crei la condivisione di file o modifichi le impostazioni di condivisione dei file nella home page. https://console.aws.amazon.com/storagegateway/

Una volta creata o aggiornata la condivisione del file per un accesso tra account e una volta caricata la condivisione file in un ambiente locale, è consigliabile testare la configurazione. È possibile eseguire questa operazione elencando contenuti directory o scrivendo file di test e accertando che i file siano visualizzati come oggetti nel bucket S3.

> **Important**
>
> Accertarsi di configurare le policy correttamente per concedere l'accesso a più account all'account utilizzato dalla condivisione file. In caso contrario, gli aggiornamenti ai file tramite le applicazioni locali non si propagano al bucket Amazon S3 con cui stai lavorando.

Resources

Per ulteriori informazioni sulle policy d'accesso e sulle liste di controllo accessi, consulta quanto segue:

Linee guida per l'utilizzo delle opzioni di policy di accesso disponibili nella Guida per l'utente di Amazon Simple Storage Service

Panoramica della lista di controllo degli accessi (ACL) nella Guida per l'utente di Amazon Simple Storage Service

Eliminare una condivisione di file

Se non è più necessaria una condivisione di file, è possibile eliminarla dalla console Storage Gateway. Quando elimini una condivisione di file, il gateway viene scollegato dal bucket Amazon S3 a cui è mappata la condivisione di file. Il bucket S3 e il relativo contenuto non vengono tuttavia eliminati.

Se il gateway sta caricando dati in un bucket S3 quando si elimina una condivisione file, il processo di eliminazione non viene completato finché non sono stati caricati tutti i dati. La condivisione file ha uno stato DELETING (ELIMINAZIONE IN CORSO) fino a quando i dati non sono stati caricati completamente.

Se non vuoi attendere che i dati vengano caricati completamente, consulta Per forzare l'eliminazione di una condivisione file più avanti in questo argomento.

Per eliminare una condivisione file

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Condivisioni di file, quindi seleziona una o più condivisioni di file da eliminare.
3. Per Actions (Operazioni), scegliere Delete file share (Elimina condivisione file). Viene visualizzata la finestra di dialogo di conferma.

4. Verifica di voler eliminare le condivisioni di file specificate, quindi digita la parola elimina nella casella di conferma e scegli Elimina.

In alcuni casi, è consigliabile non attendere che tutti i dati scritti nei file nella condivisione file NFS (Network File System) vengano caricati prima di eliminare la condivisione file. Ad esempio, potresti voler eliminare intenzionalmente dati che sono stati scritti ma non sono ancora stati caricati oppure il bucket Amazon S3 che supporta la condivisione di file potrebbe essere già stato eliminato, il che significa che il caricamento dei dati specificati non è più possibile.

In questi casi, puoi eliminare forzatamente la condivisione di file utilizzando l'operazione o l'API. Console di gestione AWS `DeleteFileShare` Questa operazione interrompe il processo di caricamento dei dati. In tal caso, la condivisione file passa allo stato FORCE_DELETING (ELIMINAZIONE_FORZATA). Per eliminare forzatamente una condivisione di file utilizzando la console Storage Gateway, vedere la procedura seguente.

Per forzare l'eliminazione di una condivisione file

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Dalla pagina dell'elenco delle condivisioni di file, scegli la condivisione di file contrassegnata per l'eliminazione nella procedura precedente per visualizzarne i dettagli. Dopo alcuni secondi, nella scheda Dettagli viene visualizzato un messaggio di notifica di eliminazione.
3. Nel messaggio che appare nella scheda Dettagli, verifica l'ID della condivisione di file che desideri eliminare forzatamente, seleziona la casella di conferma e scegli Eliminazione forzata ora.

> **Note**
>
> Non è possibile annullare l'operazione di eliminazione forzata.
> Quando elimini forzatamente una condivisione di file, parti di file parzialmente trasferite da caricamenti in più parti potrebbero rimanere su Amazon S3 dove possono comportare costi di archiviazione. Ti consigliamo di configurare una regola del ciclo di vita del bucket Amazon S3 per eliminare automaticamente queste parti di file. Per ulteriori informazioni, consulta Best practice: gestione dei caricamenti in più parti.

Puoi anche utilizzare l'operazione DeleteFileShareAPI per eliminare forzatamente la condivisione di file. L'eliminazione di una condivisione di file utilizzando l'API richiede l'autorizzazione della `storagegateway:DeleteFileShare` policy IAM.

Modifica delle impostazioni SMB per un gateway

Le impostazioni SMB a livello di gateway consentono di configurare la strategia di sicurezza, l'autenticazione Active Directory, l'accesso guest, le autorizzazioni dei gruppi locali e la visibilità della condivisione di file per le condivisioni di file SMB su un gateway.

Per modificare le impostazioni SMB a livello di gateway

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le impostazioni SMB.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli le impostazioni che desideri modificare.

Questa sezione contiene i seguenti argomenti, che forniscono informazioni e procedure aggiuntive relative alla configurazione di ciascuna delle singole impostazioni SMB per il gateway.

Argomenti

- Imposta il livello di sicurezza del gateway- Scopri come impostare un livello di sicurezza per specificare requisiti di connessione come la firma e la crittografia Server Message Block (SMB) e se consentire le connessioni dai client SMB versione 1.
- Configurare l'autenticazione di Active Directory- Scopri come configurare Active Directory aziendale o Microsoft AD AWS gestito per l'accesso autenticato dall'utente alla condivisione di file SMB.
- Fornisci l'accesso agli ospiti- Scopri come configurare il gateway per consentire l'accesso come ospite a qualsiasi utente che fornisca il nome utente e la password corretti dell'account guest.
- Configura i gruppi locali- Scopri come configurare i gruppi locali per concedere agli utenti di Active Directory autorizzazioni speciali per la condivisione di file.
- Imposta la visibilità della condivisione dei file- Scopri come specificare se le condivisioni su un gateway sono visibili quando le condivisioni vengono pubblicate dagli utenti.

Imposta un livello di sicurezza per il tuo gateway

Utilizzando un S3 File Gateway, puoi specificare un livello di sicurezza per il tuo gateway. Specificando questo livello di sicurezza, puoi impostare se il gateway deve richiedere la firma Server Message Block (SMB) o la crittografia SMB o se desideri consentire la versione 1 di SMB.

Per configurare il livello di sicurezza

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le impostazioni SMB.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli Impostazioni di sicurezza SMB.
4. Per Security level (Livello di sicurezza), selezionare una delle opzioni seguenti:

> **Note**
>
> Per informazioni sulla configurazione di questa impostazione utilizzando l' AWS API, consulta Update SMBSecurity Strategy nel riferimento API.Gateway di archiviazione AWS
> Un livello di strategia di sicurezza più elevato può influire sulle prestazioni del gateway.

- Applica AES256 la crittografia: se scegli questa opzione, S3 File Gateway consente solo connessioni da SMBv3 client che utilizzano algoritmi di crittografia AES a 256 bit. Gli algoritmi a 128 bit non sono consentiti. Questa opzione è consigliata per ambienti che gestiscono dati sensibili. Funziona con tutti gli attuali client SMB su Microsoft Windows.
- Applica la crittografia: se scegli questa opzione, S3 File Gateway consente solo le connessioni da SMBv3 client con crittografia attivata. Sono consentiti sia algoritmi a 256 bit che a 128 bit. Questa opzione è consigliata per ambienti che gestiscono dati sensibili. Funziona con tutti gli attuali client SMB su Microsoft Windows.
- Applica la firma: se scegli questa opzione, S3 File Gateway consente solo connessioni da SMBv2 o SMBv3 client con firma attivata. Questa opzione funziona con tutti i client SMB correnti su Microsoft Windows.
- Negoziato con il cliente: se si sceglie questa opzione, le richieste vengono stabilite in base a quanto negoziato dal cliente. Questa opzione è consigliata quando si desidera massimizzare la compatibilità tra i diversi client del proprio ambiente.

> **Note**
>
> Per i gateway attivati prima del 20 giugno 2019, il livello di sicurezza predefinito è Client negotiated (Negoziato dal cloud).
> Per i gateway attivati a partire dal 20 giugno 2019, il livello di sicurezza predefinito è Enforce encryption (Applica crittografia).

5. Scegli Save (Salva).

Usa Active Directory per autenticare gli utenti

Per utilizzare l'Active Directory aziendale o AWS Managed Microsoft AD per l'accesso autenticato dall'utente alla condivisione di file SMB, modifica le impostazioni SMB per il gateway con le credenziali del dominio Microsoft AD. In questo modo, il gateway può essere aggiunto al dominio di Active Directory e i membri del dominio possono accedere alla condivisione file SMB.

> **Note**
>
> Utilizzando Directory Service, è possibile creare un servizio di dominio Active Directory ospitato in. Cloud AWS
> Per utilizzarla AWS Managed Microsoft AD con un EC2 gateway Amazon, devi creare l' EC2 istanza Amazon nello stesso VPC di AWS Managed Microsoft AD, aggiungere il gruppo di sicurezza _WorkspaceMembers all'istanza EC2 Amazon e unirti al dominio AD utilizzando le credenziali di amministratore di. AWS Managed Microsoft AD
> Per ulteriori informazioni in merito, consulta la Guida all'amministrazione. AWS Managed Microsoft ADAWS Directory Service
> Per ulteriori informazioni su Amazon EC2, consulta la documentazione di Amazon Elastic Compute Cloud.

Puoi anche attivare le liste di controllo degli accessi (ACLs) sulla tua condivisione di file SMB. Per informazioni su come effettuare l'attivazione ACLs, consultaUtilizzo di Windows ACLs per limitare l'accesso alla condivisione di file SMB.

Per attivare l'autenticazione di Active Directory

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le impostazioni SMB.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli Impostazioni Active Directory.
4. Per Nome di dominio, inserisci il nome del dominio Active Directory a cui desideri che il gateway si unisca.

   > **Note**
   >
   > Active Directory status (Stato di Active Directory) mostra la voce Detached (Scollegato) quando un gateway non è mai entrato a far parte di un dominio.
   > L'account del servizio Active Directory deve disporre delle autorizzazioni necessarie. Per ulteriori informazioni, vedere Requisiti di autorizzazione dell'account del servizio Active Directory Requisiti di autorizzazione dell'.
   > L'aggiunta a un dominio crea un account computer Active Directory nel contenitore predefinito dei computer (che non è un'unità organizzativa), utilizzando l'ID Gateway del gateway come nome dell'account (ad esempio, SGW-1234ADE). Non è possibile personalizzare il nome di questo account.
   > Se l'ambiente Active Directory richiede la preconfigurazione degli account per facilitare il processo di aggiunta al dominio, sarà necessario creare questo account in anticipo.
   > Se l'ambiente Active Directory dispone di un'unità organizzativa designata per i nuovi oggetti del computer, è necessario specificare tale unità organizzativa al momento dell'accesso al dominio.
   > Se il gateway non è in grado di accedere a una directory di Active Directory, prova a connetterti con l'indirizzo IP della directory utilizzando l'operazione JoinDomainAPI.

5. Per Utente di dominio e Password di dominio, inserisci le credenziali per l'account del servizio Active Directory che il gateway utilizzerà per aggiungere il dominio.
6. (Facoltativo) Per Unità organizzativa (OU), immettere l'unità organizzativa designata utilizzata da Active Directory per i nuovi oggetti del computer.
7. (Facoltativo) Per i controller di dominio (DC), immettete il nome di uno o più DCs tramite i quali il gateway si connetterà ad Active Directory. È possibile immetterne più di uno DCs come elenco separato da virgole. Puoi lasciare vuoto questo campo per consentire al DNS di selezionare automaticamente un DC.

8. Scegli Save changes (Salva modifiche).

Per limitare l'accesso alla condivisione file a utenti e gruppi AD specifici

1. Nella console Storage Gateway, scegli la condivisione di file a cui desideri limitare l'accesso.
2. Dal menu a discesa Azioni, scegli Modifica le impostazioni di accesso alla condivisione dei file.
3. Nella sezione Accesso alla condivisione di file di utenti e gruppi, scegli le tue impostazioni.

   Per Utenti e gruppi consentiti, scegli Aggiungi utente consentito o Aggiungi gruppo consentito e inserisci un utente o un gruppo AD a cui desideri consentire l'accesso alla condivisione di file. Ripeti questa procedura per consentire il numero di utenti e gruppi necessario.

   Per Utenti e gruppi negati, scegli Aggiungi utente negato o Aggiungi gruppo negato e inserisci un utente o un gruppo AD a cui desideri negare l'accesso alla condivisione di file. Ripeti questa procedura per negare il numero di utenti e gruppi necessario.

   > **Note**
   >
   > La sezione Accesso alla condivisione di file di utenti e gruppi viene visualizzata solo se è selezionato Active Directory.
   > I gruppi devono avere il prefisso del `@` carattere. I formati accettabili includono: `DOMAIN\User1user1,@group1`, e`@DOMAIN\group1`.
   > Se si configurano gli elenchi di utenti e gruppi consentiti e negati, Windows non ACLs concederà alcun accesso che sostituisca tali elenchi.
   > Gli elenchi Utenti e gruppi consentiti e negati vengono valutati in precedenza ACLs e controllano quali utenti possono installare o accedere alla condivisione di file. Se alcuni utenti o gruppi vengono inseriti nell'elenco Consentito, l'elenco viene considerato attivo e solo tali utenti possono montare la condivisione di file.
   > Dopo che un utente ha installato una condivisione di file ACLs , offri una protezione più granulare che controlli a quali file o cartelle specifici l'utente può accedere. Per ulteriori informazioni, consulta Attivazione di Windows ACLs su una nuova condivisione di file SMB.

4. Una volta completata l'aggiunta di voci, scegliere Save (Salva).

Fornisci agli ospiti l'accesso alla tua condivisione di file

Puoi configurare S3 File Gateway per consentire l'accesso come ospite a qualsiasi utente in grado di fornire il nome utente e la password corretti dell'account guest. Se desideri che questo sia l'unico metodo con cui gli utenti possono accedere al tuo gateway di file, non è necessario aggiungere il gateway a un dominio Microsoft Active Directory. Puoi anche utilizzare questo metodo di accesso guest per creare condivisioni di file su un S3 File Gateway che è membro di un dominio Active Directory.

Quando configuri una condivisione di file per utilizzare il metodo di autenticazione Guest Access, il nome utente di accesso ospite è`smbguest`. Prima di poter creare una condivisione di file utilizzando l'accesso come ospite, è necessario modificare la password predefinita per l'`smbguest`utente.

È possibile utilizzare la procedura seguente per modificare la password dell'utente ospite`smbguest`.

Per modificare la password di accesso guest

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway dal riquadro di navigazione sul lato sinistro della pagina della console, quindi scegli il nome del gateway per il quale desideri fornire l'accesso come ospite.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli Impostazioni di accesso ospite.
4. Per Password ospite, inserisci la password di accesso ospite che desideri impostare, quindi scegli Salva modifiche.

Configura i gruppi locali per il tuo gateway

Le impostazioni dei gruppi locali consentono di concedere agli utenti o ai gruppi di Active Directory autorizzazioni speciali per le condivisioni di file SMB sul gateway.

È possibile utilizzare le impostazioni del gruppo locale per assegnare le autorizzazioni di amministratore del gateway. Gli amministratori del gateway possono utilizzare lo snap-in Cartelle condivise di Microsoft Management Console per forzare la chiusura dei file aperti e bloccati.

> **Note**
>
> È necessario aggiungere almeno un utente o un gruppo Gateway Admin prima di poter aggiungere il gateway a un dominio Active Directory.

Per assegnare Gateway Admins

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le impostazioni SMB.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli Impostazioni gruppo locale.
4. Nella sezione Impostazioni del gruppo locale, scegli le tue impostazioni. Questa sezione viene visualizzata solo per le condivisioni di file che utilizzano Active Directory.

   Per gli amministratori di Gateway, aggiungi gli utenti e i gruppi di Active Directory a cui desideri concedere le autorizzazioni di amministratore del Gateway locali. Aggiungi un utente o un gruppo per riga, incluso il nome di dominio. Ad esempio, **`corp\Domain Admins`**. Per creare righe aggiuntive, scegli Aggiungi nuovo amministratore del gateway.

   > **Note**
   >
   > Editing Gateway Admins disconnette e riconnette tutte le condivisioni di file SMB.

5. Scegli Salva modifiche, quindi scegli Procedi per confermare il messaggio di avviso visualizzato.

Imposta la visibilità della condivisione dei file

La visibilità della condivisione di file controlla se le condivisioni su un gateway sono visibili quando le condivisioni vengono pubblicate dagli utenti, ad esempio in una visualizzazione in rete o in un elenco di navigazione. Se le condivisioni di file su un gateway sono visibili, i client possono individuarle facilmente utilizzando un browser di file se conoscono l'indirizzo IP o il nome DNS del gateway. Se le condivisioni di file non sono visibili, i client devono conoscere il nome della condivisione di file oltre all'IP o al nome DNS del gateway per poter individuare le condivisioni.

> **Note**
>
> Questa impostazione non è un metodo efficace per proteggere l'accesso alle condivisioni di file nella distribuzione. Per motivi di sicurezza, consigliamo di configurare le autorizzazioni per limitare l'accesso a utenti e gruppi specifici. Per istruzioni, consulta Limitare l'accesso di utenti e gruppi per la condivisione di file SMB.

Per impostare la visibilità della condivisione di file

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le impostazioni SMB.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli Impostazioni di visibilità della condivisione dei file.
4. Per lo stato di visibilità, seleziona la casella di controllo se desideri che le condivisioni su questo gateway vengano visualizzate quando il gateway elenca le condivisioni agli utenti. Mantieni deselezionata la casella di controllo se non desideri che le condivisioni su questo gateway vengano visualizzate quando il gateway elenca le condivisioni agli utenti.

Modifica le impostazioni per la condivisione di file SMB

È possibile modificare le seguenti impostazioni per una condivisione di file SMB esistente:

- Nome di condivisione di file: scegli un nome per la condivisione di file
- Registri di controllo: attiva o disattiva i registri di controllo
- Elenco dei gruppi di log esistenti: scegli un gruppo di log esistente per i registri di controllo
- Tempo di aggiornamento della cache dei file non gateway: specifica l'intervallo con cui aggiornare la cache della condivisione di file

> **Note**
>
> L'impostazione di questo valore in un periodo inferiore a 30 minuti può influire negativamente sulle prestazioni del gateway in situazioni in cui viene spesso creato o eliminato un numero elevato di oggetti Amazon S3.

- Tempo di impostazione degli eventi di caricamento: specifica il numero di secondi di attesa dopo l'ultimo momento in cui un client ha scritto su un file prima di generare una notifica `ObjectUploaded`
- Classe di storage per nuovi oggetti: scegli una classe di storage da utilizzare per i nuovi oggetti creati nel tuo bucket Amazon S3
- Indovina il tipo MIME: scegli se vuoi che Storage Gateway indovini il tipo MIME per gli oggetti caricati in base alle estensioni di file

- File del gateway accessibili al proprietario del bucket S3: scegli se rendere i file sul gateway accessibili all' AWS account proprietario del bucket Amazon S3 collegato alla condivisione di file
- Abilita i pagamenti da parte del richiedente: scegli se richiedere agli account che leggono o richiedono dati dalla condivisione di file di pagare i costi di accesso, anziché al proprietario del bucket
- Esporta come: scegli se i file vengono esportati in stato di lettura/scrittura o di sola lettura
- Accesso a file e directory controllato da: scegli se utilizzare le autorizzazioni Windows ACLs o POSIX per controllare l'accesso a file e directory
- Blocco opportunistico (oplock): scegli se consentire alla condivisione di file di utilizzare il blocco opportunistico per ottimizzare la strategia di buffering dei file
- Forza la distinzione tra maiuscole e minuscole: scegli se il client o il gateway controllino la distinzione tra maiuscole e minuscole per i nomi di file

> **Note**
>
> Se nella condivisione di file è attualmente attivata la distinzione tra maiuscole e minuscole, la sua disattivazione potrebbe rendere inaccessibili i file con nomi identici ma maiuscole diverse (ad esempio, file.txt, File.txt). Solo una versione rimarrà accessibile ai client senza distinzione tra maiuscole e minuscole.

- Enumerazione basata sull'accesso per file e directory: scegli se rendere visibili i file e le cartelle della condivisione a tutti gli utenti durante l'enumerazione delle directory o solo agli utenti con accesso in lettura

> **Note**
>
> Non è possibile modificare una condivisione di file esistente in modo che punti a un nuovo bucket o punto di accesso o modificare le impostazioni dell'endpoint VPC. È possibile configurare tali impostazioni solo quando si crea una nuova condivisione di file.

Per modificare le impostazioni della condivisione file

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file da aggiornare.
3. Per Azioni, scegli Modifica le impostazioni di condivisione dei file.

4. Modifica le impostazioni che desideri modificare.
5. Scegli Save (Salva).

Limita l'accesso di utenti e gruppi alla condivisione di file SMB

Ti consigliamo di aggiungere utenti o gruppi consentiti o negati per limitare l'accesso alla condivisione di file. In caso contrario, la condivisione di file sarà disponibile per tutti gli utenti autenticati.

Per modificare le impostazioni di accesso SMB

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Condivisioni di file, quindi scegli la condivisione di file SMB che desideri modificare.
3. Per Azioni, scegli Modifica le impostazioni di accesso alla condivisione di file.
4. Nella sezione Accesso alla condivisione di file di utenti e gruppi, scegli le tue impostazioni.

   Per Utenti e gruppi consentiti, scegli Aggiungi utente consentito o Aggiungi gruppo consentito e inserisci un utente o un gruppo AD a cui desideri consentire l'accesso alla condivisione di file. Ripeti questa procedura per consentire il numero di utenti e gruppi necessario. A tutti gli utenti non presenti nell'elenco Utenti e gruppi consentiti verrà negato l'accesso.

   Per Utenti e gruppi negati, scegli Aggiungi utente negato o Aggiungi gruppo negato e inserisci un utente o un gruppo AD a cui desideri negare l'accesso alla condivisione di file. Ripeti questa procedura per negare il numero di utenti e gruppi necessario. Se l'elenco Utenti e gruppi consentiti è vuoto, verrà concesso l'accesso a tutti gli utenti diversi da quelli presenti nell'elenco Utenti e gruppi negati.

   > **Note**
   >
   > Immettere solo il nome dell'utente o del gruppo AD. Il nome di dominio è implicito nell'appartenenza del gateway all'AD specifico a cui è collegato il gateway.
   > Se non specifichi utenti o gruppi autorizzati o negati, qualsiasi utente AD autenticato può esportare la condivisione di file.

Modifica il metodo di crittografia lato server per una condivisione di file esistente

La procedura seguente descrive come modificare il metodo di crittografia lato server per una condivisione di file NFS o SMB esistente utilizzando la console Storage Gateway. Per eseguire questa azione utilizzando l'API Storage Gateway, vedere Update NFSFile Share o Update SMBFile Share nel riferimento all'API AWS Storage Gateway.

> **Note**
>
> L'aggiornamento del metodo di crittografia applica il nuovo metodo agli oggetti esistenti archiviati nei bucket Amazon S3 dopo l'aggiornamento.
> Se configuri File Gateway per utilizzare SSE-KMS per la crittografia, devi aggiungere manualmente,`kms:Encrypt`, `kms:Decrypt` `kms:ReEncrypt*` `kms:GenerateDataKey`, e `kms:DescribeKey` le autorizzazioni al ruolo IAM associato alla condivisione di file. Per ulteriori informazioni, consulta Using Identity-Based Policies (IAM Policies) for Storage Gateway.

Per modificare il metodo di crittografia lato server per una condivisione di file NFS o SMB

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Condivisioni di file, quindi scegli la condivisione di file per la quale desideri modificare il metodo di crittografia.
3. Per Azioni, scegli Modifica la crittografia della condivisione di file.
4. Per la crittografia, scegli il tipo di crittografia che desideri utilizzare per i file inattivi in Amazon S3:

   - Per utilizzare la crittografia lato server gestita con Amazon S3 (SSE-S3), scegli S3 Managed Keys (SSE-S3). Per ulteriori informazioni, consulta Usare la crittografia lato server con le chiavi gestite di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.
   - Per utilizzare la crittografia lato server gestita con AWS Key Management Service (SSE-KMS), scegli KMS-Managed Keys (SSE-KMS). Per la chiave KMS primaria, scegli una chiave KMS esistente o scegli Crea una nuova chiave AWS KMS per creare una nuova chiave KMS nella console del servizio di gestione delle chiavi (). AWS AWS KMS

     Per ulteriori informazioni su AWS KMS, consulta Cos'è AWS il servizio di gestione delle chiavi? nella Guida per gli AWS Key Management Service sviluppatori.

- Per utilizzare la crittografia lato server a doppio livello gestita con AWS Key Management Service (DSSE-KMS), scegli la crittografia lato server a doppio livello con chiavi (DSSE-KMS). AWS Key Management Service Per la chiave KMS primaria, scegli una chiave KMS esistente o scegli Crea una nuova chiave AWS KMS per creare una nuova chiave KMS nella console Key Management Service (). AWS AWS KMS

  Per ulteriori informazioni su DSSE-KMS, consulta Uso della crittografia lato server a doppio livello con chiavi AWS KMS nella Guida per l'utente di Amazon Simple Storage Service.

  > **Note**
  >
  > Sono previsti costi aggiuntivi per l'utilizzo di DSSE-KMS e delle chiavi. AWS KMS Per ulteriori informazioni, consultare Prezzi di AWS KMS.
  > Per specificare una AWS KMS chiave con un alias non presente nell'elenco o per utilizzare una AWS KMS chiave di un AWS account diverso, è necessario utilizzare il. AWS Command Line Interface Le chiavi KMS asimmetriche non sono supportate. Per ulteriori informazioni, vedere Create SMBFile Share nello AWS Storage Gateway API Reference.

5. Al termine, scegli Salva le modifiche.

Modifica le impostazioni per la condivisione di file NFS

Utilizzare la procedura seguente per modificare le impostazioni per una condivisione di file NFS esistente dopo averla creata.

> **Note**
>
> Non è possibile modificare una condivisione di file esistente in modo che punti a un nuovo bucket o punto di accesso o modificare le impostazioni dell'endpoint VPC. È possibile configurare tali impostazioni solo quando si crea una nuova condivisione di file.

Per modificare le impostazioni della condivisione file

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file da aggiornare.

3. Per Azioni, scegli Modifica le impostazioni di condivisione dei file.
4. Per Nome condivisione file, inserisci un nome per la condivisione di file.
5. Per i registri di controllo, seleziona una delle seguenti opzioni:

   - Per creare un nuovo gruppo di log per questa condivisione di file, scegli Crea un nuovo gruppo di log.
   - Per inviare notifiche sullo stato e sulle risorse relative a questa condivisione di file a un gruppo di log esistente, scegli Usa un gruppo di log esistente, quindi scegli il gruppo desiderato dall'elenco.
   - Per disattivare la registrazione per questa condivisione di file, scegli Disattiva registrazione.

   Per ulteriori informazioni sui log di controllo, consulta Understanding S3 File Gateway audit logs.
6. Per il tempo di aggiornamento della cache dei file non Gateway, scegli Imposta intervallo di aggiornamento, quindi imposta il tempo in minuti o giorni per aggiornare la cache della condivisione di file utilizzando Time To Live (TTL). TTL è il periodo di tempo trascorso dall'ultimo aggiornamento. Trascorso l'intervallo TTL, l'accesso a una directory fa sì che File Gateway aggiorni i contenuti di quella directory dal bucket Amazon S3.

   > **Note**
   >
   > L'impostazione di questo valore in un periodo inferiore a 30 minuti può influire negativamente sulle prestazioni del gateway in situazioni in cui viene spesso creato o eliminato un numero elevato di oggetti Amazon S3.
7. Per Tempo di impostazione degli eventi di caricamento, scegli Imposta tempo di assestamento, quindi inserisci il tempo di impostazione in secondi. Il tempo di impostazione controlla il ritardo minimo tra l'ultima operazione di scrittura del client e la generazione della notifica di registro. `ObjectUploaded` Poiché i client possono eseguire molte piccole scritture su file in breve tempo, consigliamo di impostare questo parametro il più a lungo possibile per evitare di generare più notifiche per lo stesso file in rapida successione. Per ulteriori informazioni, consulta Ricevere una notifica di caricamento di file.
8. Per Classe di archiviazione per nuovi oggetti, scegli una classe di archiviazione dall'elenco a discesa. Per ulteriori informazioni sulle classi di archiviazione, consulta Utilizzo delle classi di archiviazione con un File Gateway.
9. In Metadati degli oggetti, procedi come segue:

a. Seleziona Indovina il tipo MIME se desideri consentire a Storage Gateway di indovinare il tipo di file multimediale per gli oggetti caricati in base alle relative estensioni di file.

b. Seleziona i file Gateway accessibili al proprietario del bucket S3, se desideri che l' AWS account proprietario del bucket S3 abbia la piena proprietà dei file creati dal gateway, incluse le autorizzazioni di lettura, scrittura, modifica ed eliminazione.

10. Seleziona Enable requester pay se desideri che sia il richiedente del file anziché il proprietario del bucket a pagare il costo della richiesta di dati e del download dal bucket S3.

11.

12. Per il livello di accesso, scegli una delle seguenti opzioni:

    - Root squash (default) (Squash root - impostazione predefinita): l'accesso per il superuser remoto (root) è mappato a UID (65534) e GID (65534).
    - All squash (Squash completo): gli accessi di tutti gli utenti sono mappati all'ID utente (UID) (65534) e all'ID gruppo (GID) (65534).
    - No root squash (Nessuno squash root): il superuser remoto (root) riceve l'accesso come root.

13. Per Esporta come, seleziona una delle seguenti opzioni:

    - Per consentire ai client di leggere e scrivere file sulla condivisione di file, seleziona Lettura/scrittura.
    - Per consentire ai client di leggere i file ma non di scrivere nella condivisione di file, seleziona Sola lettura.

    > **Note**
    >
    > Per le condivisioni di file montate su un client Microsoft Windows, se si sceglie Sola lettura, è possibile che venga visualizzato un messaggio relativo a un errore imprevisto che impedisce di creare la cartella. Ignorare questo messaggio.

14. Quando hai finito di modificare le impostazioni, scegli Salva modifiche.

Modifica le impostazioni predefinite dei metadati per la condivisione di file NFS

Se non imposti i valori dei metadati per i file o le directory nel bucket, S3 File Gateway imposta i valori dei metadati predefiniti. Questi valori includono le autorizzazioni Unix per file e cartelle. È possibile modificare le impostazioni predefinite dei metadati sulla console Storage Gateway.

Quando il tuo S3 File Gateway archivia file e cartelle in Amazon S3, i permessi dei file Unix vengono archiviati nei metadati degli oggetti. Quando S3 File Gateway rileva oggetti che non sono stati archiviati da S3 File Gateway, a questi oggetti vengono assegnate le autorizzazioni di file Unix predefinite. Le autorizzazioni Unix predefinite sono indicate nella tabella seguente.

Metadati	Description
Autorizzazioni directory	Modalità di directory Unix nel formato "nnnn". Ad esempio, "0666" rappresenta la modalità di accesso per tutte le directory all'interno della condivisione file. Il valore predefinito è 0777.
Autorizzazioni di file	Modalità di file Unix nel formato "nnnn". Ad esempio, "0666" rappresenta la modalità di file all'interno della condivisione file. Il valore predefinito è 0666.
ID utente	ID del proprietario predefinito per i file nella condivisione file. Il valore predefinito è 65534.
ID gruppo	ID del gruppo predefinito per la condivisione file. Il valore predefinito è 65534.

Per modificare le impostazioni predefinite dei metadati

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file da aggiornare.
3. Per Actions (Operazioni), scegliere Edit file metadata defaults (Modifica le impostazioni predefinite dei metadati dei file).

4. Nella finestra di dialogo Edit file metadata defaults (Modifica le impostazioni predefinite dei metadati dei file) specificare le informazioni dei metadati e scegliere Save (Salva).

Limita l'accesso dei client alla condivisione di file NFS

Si consiglia di modificare le impostazioni di accesso al client NFS per definire un elenco di indirizzi IP client specifici o intervalli di blocchi CIDR per i client NFS autorizzati a connettersi alla condivisione di file NFS. Se scegli di non limitare l'accesso, qualsiasi client della tua rete può eseguire il montaggio sulla tua condivisione di file.

Per limitare l'accesso dei client alla condivisione di file NFS

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Condivisioni di file dal riquadro di navigazione sul lato sinistro della pagina della console, quindi scegli l'ID di condivisione file della condivisione di file NFS che desideri modificare.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni di accesso alla condivisione di file.

   La sezione Oggetti di accesso mostra un elenco di indirizzi IP e blocchi CIDR attualmente autorizzati a connettersi alla condivisione di file NFS. Se l'accesso non è attualmente limitato, verrà visualizzata una voce in Client consentiti per il blocco CIDR 0.0.0.0/0, che indica che tutti gli indirizzi possibili possono connettersi. IPv4
4. In Client consentiti, a destra del blocco CIDR 0.0.0.0/0, scegli Rimuovi.
5. Scegli Aggiungi client, quindi fornisci un indirizzo IP o un intervallo di indirizzi in notazione CIDR per i client che desideri consentire.
6. Ripeti il passaggio precedente per aggiungere altri indirizzi IP o intervalli, se necessario. Se commetti un errore o devi revocare l'accesso, puoi scegliere Rimuovi a destra dell'indirizzo IP o dell'intervallo che desideri eliminare dall'elenco.
7. Al termine, scegli Salva modifiche.

Aggiornamento della cache degli oggetti del bucket Amazon S3

Mentre il client NFS o SMB esegue le operazioni del file system, il gateway mantiene un inventario degli oggetti nella cache degli oggetti di Amazon S3 associata alla condivisione di file. Il tuo gateway utilizza questo inventario memorizzato nella cache per ridurre la latenza e la frequenza delle richieste Amazon S3. Questa operazione non importa file nella memoria cache di S3 File Gateway. Aggiorna

solo l'inventario memorizzato nella cache per riflettere le modifiche nell'inventario degli oggetti nella cache degli oggetti di Amazon S3.

Per aggiornare la cache degli oggetti del bucket S3 per la condivisione di file, seleziona il metodo più adatto al tuo caso d'uso dall'elenco seguente, quindi completa la procedura corrispondente riportata di seguito.

> **Note**
>
> Indipendentemente dal metodo utilizzato, l'elenco di una directory per la prima volta la inizializza, il che fa sì che il gateway elenchi i contenuti dei metadati della directory da Amazon S3. Il tempo necessario per inizializzare una directory è proporzionale al numero di voci in quella directory.

Argomenti

- Configurare una pianificazione di aggiornamento automatico della cache utilizzando la console Storage Gateway
- Configura una pianificazione di aggiornamento automatico della cache utilizzando AWS Lambda una regola Amazon CloudWatch
- Eseguire un aggiornamento manuale della cache utilizzando la console Storage Gateway
- Eseguire un aggiornamento manuale della cache utilizzando l'API Storage Gateway

Configurare una pianificazione di aggiornamento automatico della cache utilizzando la console Storage Gateway

La procedura seguente configura una pianificazione di aggiornamento automatico della cache basata su un valore Time To Live (TTL) specificato dall'utente. Prima di configurare una pianificazione di aggiornamento della cache basata su TTL, considerate quanto segue:

- Il TTL viene misurato come il periodo di tempo trascorso dall'ultimo aggiornamento della cache per una determinata directory.
- L'aggiornamento della cache basato su TTL si verifica solo quando si accede a una determinata directory dopo la scadenza del periodo TTL specificato.
- L'aggiornamento non è ricorsivo. Si verifica solo nelle directory specifiche a cui si accede.

- L'aggiornamento comporta i costi dell'API Amazon S3 solo per le directory che non sono state sincronizzate dalla scadenza del TTL.
  - Le directory vengono sincronizzate solo se vi si accede tramite attività NFS o SMB.
  - La sincronizzazione non si verifica più frequentemente del periodo TTL specificato.
- La configurazione dell'aggiornamento della cache basato su TTL è consigliata solo se aggiorni frequentemente il contenuto del tuo bucket Amazon S3 direttamente, al di fuori del flusso di lavoro tra il gateway e il bucket Amazon S3.
- Le operazioni NFS e SMB che accedono alle directory con dati scaduti TTLs verranno bloccati mentre il gateway aggiorna il contenuto della directory.

> **Note**
>
> Poiché l'aggiornamento della cache può bloccare le operazioni di accesso alle directory, consigliamo di configurare il periodo TTL più lungo possibile per l'implementazione.

Per configurare una pianificazione automatica dell'aggiornamento della cache utilizzando la console Storage Gateway

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Condivisioni di file.
3. Scegli la condivisione di file per la quale desideri configurare la pianificazione dell'aggiornamento.
4. Per Azioni, scegli Modifica le impostazioni di condivisione dei file.
5. Per l'aggiornamento automatico della cache da S3 dopo, seleziona la casella di controllo e imposta l'ora in giorni, ore e minuti per aggiornare la cache della condivisione di file utilizzando Time To Live (TTL). TTL è il periodo di tempo trascorso dall'ultimo aggiornamento dopo il quale l'accesso alla directory farebbe sì che File Gateway aggiorni per la prima volta i contenuti di quella directory dal bucket Amazon S3.
6. Scegli Save changes (Salva modifiche).

Configura una pianificazione di aggiornamento automatico della cache utilizzando AWS Lambda una regola Amazon CloudWatch

Per configurare una pianificazione di aggiornamento automatico della cache utilizzando AWS Lambda una regola Amazon CloudWatch

1. Identifica il bucket S3 utilizzato da S3 File Gateway.
2. Verifica che la sezione Evento sia vuota. Si popola automaticamente in un secondo momento.
3. Crea un ruolo IAM e consenti Trust Relationship for `lambda.amazonaws.com` Lambda.
4. Utilizza la seguente politica.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Crea una funzione Lambda dalla console Lambda.
6. Usa la seguente funzione per l'attività Lambda.

```
import json
```

```
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406474878:share/
share-E51FBS9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. Per il ruolo Execution, scegli il ruolo IAM che hai creato.
8. Facoltativo: aggiungi un trigger per Amazon S3 e seleziona l'evento ObjectCreatedo. ObjectRemoved

> **Note**
>
> `RefreshCache`deve completare un processo prima di iniziarne un altro. Quando si creano o si eliminano molti oggetti in un bucket, le prestazioni potrebbero peggiorare. Pertanto, sconsigliamo di utilizzare i trigger S3. Utilizza invece la CloudWatch regola Amazon descritta di seguito.

9. Crea una CloudWatch regola sulla CloudWatch console e aggiungi una pianificazione. In genere, consigliamo una tariffa fissa di 30 minuti. Tuttavia, puoi utilizzare 1—2 ore su un bucket S3 di grandi dimensioni.
10. Aggiungi un nuovo trigger per CloudWatch gli eventi e scegli la regola che hai appena creato.
11. Salva la tua configurazione Lambda. Scegli Test (Esegui test).
12. Scegli S3 PUT e personalizza il test in base alle tue esigenze.
13. Il test dovrebbe avere esito positivo. In caso contrario, modifica il JSON in base alle tue esigenze e ripeti il test.
14. Apri la console Amazon S3 e verifica che l'evento creato e l'ARN della funzione Lambda siano presenti.
15. Carica un oggetto nel tuo bucket S3 utilizzando la console Amazon S3 o il. AWS CLI

    La CloudWatch console genera un CloudWatch output simile al seguente.

```
{
    u'Records': [
```

```
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::amzn-s3-demo-bucket', u'name':
 u'MY-GATEWAY-NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}},
 u's3SchemaVersion': u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

L'invocazione Lambda fornisce un output simile al seguente.

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

La condivisione NFS montata sul client rifletterà questo aggiornamento.

> **Note**
>
> Per le cache che aggiornano la creazione o l'eliminazione di oggetti di grandi dimensioni in bucket di grandi dimensioni con milioni di oggetti, gli aggiornamenti potrebbero richiedere ore.

16. Elimina l'oggetto manualmente utilizzando la console Amazon S3 o. AWS CLI

17. Visualizza la condivisione NFS montata sul tuo client. Verifica che l'oggetto sia sparito (perché la cache è stata aggiornata).
18. Controlla i CloudWatch log per vedere il registro dell'eliminazione con l'evento. `ObjectRemoved:Delete`

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
}
```

> **Note**
>
> Per i cron job o le attività pianificate, il tuo evento di CloudWatch registro è. `u'detail-type': u'Scheduled Event'`

Eseguire un aggiornamento manuale della cache utilizzando la console Storage Gateway

Per eseguire un aggiornamento manuale della cache utilizzando la console Storage Gateway

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Condivisioni di file, quindi scegli la condivisione di file per la quale desideri eseguire l'aggiornamento.
3. Per Actions (Operazioni), scegliere Refresh cache (Aggiorna cache).

   Il tempo richiesto dal processo di aggiornamento dipende dal numero di oggetti memorizzati nella cache del gateway e dal numero di oggetti che sono stati aggiunti o rimossi dal bucket S3.

Eseguire un aggiornamento manuale della cache utilizzando l'API Storage Gateway

La procedura seguente esegue un aggiornamento manuale della cache utilizzando l'API Storage Gateway. Prima di eseguire un aggiornamento della cache basato su API, considera quanto segue:

- È possibile specificare un aggiornamento ricorsivo o non ricorsivo.
- Un aggiornamento ricorsivo richiede più risorse e più costoso.
- L'aggiornamento comporta i costi dell'API Amazon S3 solo per le directory passate come argomenti nella richiesta e per i discendenti di tali directory se si specifica un aggiornamento ricorsivo.
- L'aggiornamento viene eseguito contemporaneamente ad altre operazioni mentre il gateway è in uso.
  - Le operazioni NFS e SMB in genere non vengono bloccate durante gli aggiornamenti, a meno che non sia attivo un aggiornamento per la directory a cui l'operazione accede.
  - Il gateway non è in grado di determinare se il contenuto corrente della cache è obsoleto e utilizza il contenuto corrente per le operazioni NFS e SMB indipendentemente dall'aggiornamento.
  - Poiché l'aggiornamento della cache utilizza risorse hardware virtuali del gateway, le prestazioni del gateway potrebbero subire un impatto negativo durante l'aggiornamento.
- L'aggiornamento della cache basato su API è consigliato solo se aggiorni il contenuto del bucket Amazon S3 direttamente, al di fuori del flusso di lavoro tra il gateway e il bucket Amazon S3.

> **Note**
>
> Se conosci le directory specifiche in cui stai aggiornando i contenuti di Amazon S3 al di fuori del flusso di lavoro del gateway, ti consigliamo di specificare queste directory nella richiesta di aggiornamento basata su API per ridurre i costi delle API di Amazon S3 e l'impatto sulle prestazioni del gateway.

Per eseguire un aggiornamento manuale della cache utilizzando l'API Storage Gateway

- Invia una richiesta HTTP POST per richiamare l'`RefreshCache`operazione con i parametri desiderati tramite l'API Storage Gateway. Per ulteriori informazioni, vedere RefreshCache AWSlo Storage Gateway API Reference.

> **Note**
>
> L'invio della `RefreshCache` richiesta avvia solo l'operazione di aggiornamento della cache. Quando l'aggiornamento della cache termina, non significa necessariamente l'aggiornamento dei file sia stato completato. Per stabilire se l'operazione di aggiornamento dei file sia completa prima di verificare la presenza di nuovi file sulla condivisione file del gateway, utilizzare la notifica `refresh-complete`. A tale scopo,

puoi iscriverti per ricevere notifiche tramite un CloudWatch evento Amazon. Per ulteriori informazioni, consulta Ricevere notifiche sulle operazioni sui file.

Utilizzo di S3 Object Lock con Amazon S3 File Gateway

Amazon S3 File Gateway supporta l'accesso ai bucket S3 con Amazon S3 Object Lock attivato. Amazon S3 Object Lock consente di archiviare oggetti utilizzando un modello «Write Once Read Many» (WORM). Quando usi Amazon S3 Object Lock, puoi impedire che un oggetto nel tuo bucket S3 venga eliminato o sovrascritto. Amazon S3 Object Lock collabora con il controllo delle versioni degli oggetti per proteggere i dati.

Se attivi Amazon S3 Object Lock, puoi comunque modificare l'oggetto. Ad esempio, può essere scritto, eliminato o rinominato tramite una condivisione di file su un S3 File Gateway. Quando modifichi un oggetto in questo modo, S3 File Gateway inserisce una nuova versione dell'oggetto senza influire sulla versione precedente (ovvero l'oggetto bloccato).

Ad esempio, se si utilizza l'interfaccia NFS o SMB di S3 File Gateway per eliminare un file e l'oggetto S3 corrispondente è bloccato, il gateway inserisce un marker di eliminazione S3 come versione successiva dell'oggetto e lascia invariata la versione originale dell'oggetto. Allo stesso modo, se un S3 File Gateway modifica il contenuto o i metadati di un oggetto bloccato, viene caricata una nuova versione dell'oggetto con le modifiche, ma la versione originale bloccata dell'oggetto rimane invariata.

Per ulteriori informazioni su Amazon S3 Object Lock, consulta Bloccare oggetti usando S3 Object Lock nella Guida per l'utente di Amazon Simple Storage Service.

Comprendere lo stato della condivisione dei file

Puoi visualizzare lo stato di salute di una condivisione di file a colpo d'occhio esaminandone lo stato. Se lo stato indica che la condivisione di file funziona normalmente, non è necessaria alcuna azione da parte dell'utente. Se lo stato indica che c'è un problema, puoi indagare per determinare se è necessario intervenire.

È possibile visualizzare lo stato di una condivisione di file sulla console Storage Gateway nella colonna Stato. Una condivisione di file che funziona correttamente mostra lo stato DISPONIBILE. Questo dovrebbe essere lo stato per la maggior parte del tempo.

La tabella seguente descrive gli stati delle condivisioni di file, il loro significato e se potrebbe essere necessaria un'azione.

Status	Significato
DISPONIBILE	La condivisione file è configurata correttamente ed è disponibile per l'uso. Questo è lo stato standard per una condivisione di file che funziona correttamente.
CREAZIONE IN CORSO	La condivisione di file non è ancora stata creata completamente e non è pronta per l'uso. Lo stato CREATING (CREAZIONE IN CORSO) è transitorio. Nessuna operazione richiesta. Se la condivisione di file rimane bloccata in questo stato, probabilmente è perché la VM gateway ha perso la connessione a AWS.
AGGIORNAMENTO IN CORSO	La configurazione della condivisione di file è attualmente in fase di aggiornamento. Lo stato UPDATING è transitorio. Nessuna operazion e richiesta. Se una condivisione di file rimane bloccata in questo stato, probabilmente è perché la macchina virtuale gateway ha perso la connessione a. AWS
ELIMINAZIONE IN CORSO	È in corso l'eliminazione della condivisione file. La condivisione di file non viene eliminata finché tutti i dati non vengono caricati su. AWS Lo stato DELETING (ELIMINAZIONE IN CORSO) è transitorio e non è richiesta alcuna operazione.
FORCE_DEL ETING (ELIMINAZ IONE_FORZATA)	È in corso l'eliminazione forzata della condivisione file. La condivisione di file viene eliminata immediatamente e i dati non vengono caricati su AWS. Lo stato FORCE_DELETING (ELIMINAZIONE_FORZATA) è transitorio e non è richiesta alcuna operazione.
NON DISPONIBILE	La condivisione file si trova in uno stato non integro. È richiesta un'azione . Alcune possibili cause includono errori nelle policy relative ai ruoli o la mappatura su un bucket Amazon S3 che non esiste. Quando il problema che ha causato lo stato di malfunzionamento viene risolto, la condivisi one di file torna allo stato AVAILABLE.

Comprendere lo stato del gateway

A ogni gateway nell'implementazione AWS di Storage Gateway è associato uno stato che indica a colpo d'occhio lo stato del gateway. Nella maggior parte dei casi, lo stato indica che il gateway funziona normalmente e che non è necessaria alcuna azione da parte dell'utente. In alcuni casi, lo stato indica un problema che potrebbe richiedere un'operazione da parte tua.

È possibile visualizzare lo stato di ogni gateway nella distribuzione nella pagina Gateway della console Storage Gateway. Lo stato del gateway viene visualizzato nella colonna Stato accanto al nome del gateway. Un gateway che funziona normalmente ha lo stato di`RUNNING`.

Nella tabella seguente, è possibile trovare una descrizione dello stato di ogni gateway e l'opportunità di agire in base allo stato. Un gateway deve avere `RUNNING` lo stato per tutto o per la maggior parte del tempo in cui è in uso.

Status	Significato
`RUNNING`	Il gateway è configurato correttamente ed è disponibile per l'uso.
`OFFLINE`	Il gateway potrebbe essere in uno `OFFLINE` stato attivo per uno o più dei seguenti motivi: • Il gateway non può raggiungere gli endpoint del servizio Storage Gateway. • Il gateway ha avuto un arresto imprevisto. • Al gateway è associato un disco di cache che è disconnesso, è stato modificato o ha avuto un errore.

Gestione della larghezza di banda per Amazon S3 File Gateway

È possibile limitare la velocità di upload dal gateway per AWS controllare la quantità di larghezza di banda di rete utilizzata dal gateway. Per impostazione predefinita, un gateway attivato non ha limiti di velocità.

È possibile configurare una bandwidth-rate-limit pianificazione utilizzando un AWS Software Development Kit (SDK) o l' Gateway di archiviazione AWS API (vedere UpdateBandwidthRateLimitScheduleIo AWS Storage Gateway API Reference). Console di gestione

AWS Utilizzando una pianificazione dei limiti di velocità di larghezza di banda, è possibile configurare i limiti in modo che cambino automaticamente nel corso del giorno o della settimana. Per ulteriori informazioni, consulta Visualizza e modifica la bandwidth-rate-limit pianificazione del gateway utilizzando la console Storage Gateway.

Puoi monitorare la velocità di caricamento del gateway utilizzando la `CloudBytesUploaded` metrica nella scheda Monitoraggio nella console Storage Gateway o in Amazon. CloudWatch

> **Note**
>
> I limiti di velocità della larghezza di banda si applicano solo ai caricamenti di file di Storage Gateway. Le altre operazioni del gateway non sono influenzate.
> La limitazione della velocità di larghezza di banda funziona bilanciando la velocità effettiva di tutti i file caricati, calcolata in media su ogni secondo. Sebbene sia possibile che i caricamenti superino brevemente il limite di velocità della larghezza di banda per un microsecondo o millisecondo specifico, in genere ciò non comporta picchi elevati per periodi di tempo più lunghi.
> La configurazione dei limiti e delle pianificazioni della velocità di larghezza di banda non è attualmente supportata per il tipo Amazon FSx File Gateway.

Argomenti

- Visualizza e modifica la bandwidth-rate-limit pianificazione del gateway utilizzando la console Storage Gateway
- Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK per Java
- Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK per .NET
- Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS Tools for Windows PowerShell

Visualizza e modifica la bandwidth-rate-limit pianificazione del gateway utilizzando la console Storage Gateway

In questa sezione viene descritto come visualizzare e modificare la pianificazione dei limiti di velocità della larghezza di banda per il gateway.

Per visualizzare e modificare la pianificazione del limite di velocità della larghezza di banda

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione di sinistra, scegliere Gateway e quindi scegliere il gateway da gestire.
3. Per Operazioni, scegliere Modifica pianificazione del limite di velocità di larghezza di banda.

   La bandwidth-rate-limit pianificazione corrente del gateway viene visualizzata nella pagina Modifica pianificazione del limite di velocità di larghezza di banda. Per impostazione predefinita, un nuovo gateway non ha limiti di velocità di larghezza di banda definiti.
4. (Facoltativo) Scegli Aggiungi nuovo limite di velocità di larghezza di banda per aggiungere un nuovo intervallo configurabile alla pianificazione. Per ogni intervallo aggiunto, inserisci le seguenti informazioni:

   - Velocità di caricamento: inserisci il limite di velocità di caricamento, in megabit al secondo (Mbps). Il valore minimo è 100 Mbps.
   - Giorni della settimana: seleziona il giorno o i giorni di ogni settimana in cui desideri applicare l'intervallo. È possibile applicare l'intervallo nei giorni feriali (dal lunedì al venerdì), nei fine settimana (sabato e domenica), tutti i giorni della settimana o in un giorno specifico della settimana. Per applicare il limite di velocità di larghezza di banda in modo uniforme e costante in tutti i giorni e in ogni momento, scegli Nessuna pianificazione.
   - Ora di inizio: inserisci l'ora di inizio per l'intervallo di larghezza di banda, utilizzando il formato HH:MM e lo scostamento del fuso orario rispetto all'UTC per il gateway.

     > **Note**
     >
     > L' bandwidth-rate-limitintervallo inizia all'inizio del minuto specificato qui.

   - Ora di fine: inserisci l'ora di fine dell'intervallo di larghezza di banda, utilizzando il formato HH:MM e lo scostamento del fuso orario rispetto al GMT per il gateway.

     > **Important**
     >
     > L' bandwidth-rate-limitintervallo termina alla fine del minuto specificato qui. Per pianificare un intervallo che termini alla fine di un'ora, immettere. **59**

Per programmare intervalli continui consecutivi, con transizione all'inizio dell'ora, senza interruzioni tra gli intervalli, inserite **59** il minuto finale del primo intervallo. Inserisci **00** per il minuto di inizio dell'intervallo successivo.

5. (Facoltativo) Ripeti il passaggio precedente, se necessario, fino al completamento della bandwidth-rate-limit pianificazione. Se occorre eliminare un intervallo dalla pianificazione, scegli Rimuovi.

> **Important**
>
> Bandwidth-rate-limitgli intervalli non possono sovrapporsi. L'ora di inizio di un intervallo deve essere successiva all'ora di fine di un intervallo precedente, e precedente all'ora di inizio di un intervallo successivo.

6. Al termine, scegli Salva modifiche.

Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK per Java

Aggiornando i limiti di velocità di larghezza di banda a livello di programmazione, è possibile modificare tali limiti automaticamente per un periodo di tempo, ad esempio utilizzando attività pianificate. L'esempio seguente illustra come aggiornare i limiti di velocità della larghezza di banda di un gateway usando AWS SDK per Java. Per usare il codice di esempio, devi avere familiarità con l'esecuzione di un'applicazione di console Java. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di AWS SDK per Java .

Example : Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK per Java

L'esempio di codice Java seguente aggiorna i limiti di velocità della larghezza di banda di un gateway. Per utilizzare questo codice di esempio, devi fornire l'endpoint del servizio, il gateway Amazon Resource Name (ARN) e il limite di upload. Per un elenco degli endpoint del servizio AWS che è possibile utilizzare con Storage Gateway, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
```

```
   import com.amazonaws.auth.PropertiesCredentials;
   import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

       // The gatewayARN
       public static String gatewayARN = "*** provide gateway ARN ***";

       // The endpoint
       static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

       // Rates
       static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

       public static void main(String[] args) throws IOException {

           // Create a Storage Gateway client
           sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
           sgClient.setEndpoint(serviceURL);

           UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File Gateways

       }

       private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
           try
           {
               BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
```

```
                BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

                String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
                System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
                System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
            }
            catch (AmazonClientException ex)
            {
                System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
            }
        }
    }
```

Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK per .NET

Aggiornando i limiti di velocità di larghezza di banda a livello di programmazione, è possibile modificare tali limiti automaticamente per un periodo di tempo, ad esempio utilizzando attività pianificate. L'esempio seguente dimostra come aggiornare i limiti di velocità di larghezza di banda di un gateway utilizzando il Software Development Kit (SDK) per .NET. AWS Per usare il codice di

esempio, devi avere familiarità con l'esecuzione di un'applicazione di console .NET. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di AWS SDK per .NET .

Example : Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK per .NET

L'esempio di codice C# seguente aggiorna i limiti di velocità della larghezza di banda di un gateway. Per utilizzare questo codice di esempio, devi fornire l'endpoint del servizio, il gateway Amazon Resource Name (ARN) e il limite di upload. Per un elenco degli endpoint del servizio AWS che è possibile utilizzare con Storage Gateway, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.

```
    using System;
    using System.Collections.Generic;
    using System.Linq;
    using System.Text;
    using Amazon.StorageGateway;
    using Amazon.StorageGateway.Model;

    namespace AWSStorageGateway
    {
        class UpdateBandwidthExample
        {
            static AmazonStorageGatewayClient sgClient;
            static AmazonStorageGatewayConfig sgConfig;

            // The gatewayARN
            public static String gatewayARN = "*** provide gateway ARN ***";

            // The endpoint
            static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";

            // Rates
            static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a Storage Gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);
```

```
                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
            }

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                  bandwidthRateLimitIntervals.Add(noScheduleInterval);
                  UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

                    UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                    String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                    Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                    Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
                }
                catch (AmazonStorageGatewayException ex)
                {
```

```
                    Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
                }
            }
        }
    }
```

Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS Tools for Windows PowerShell

Aggiornando i limiti di velocità di larghezza di banda a livello di programmazione, è possibile modificare tali limiti automaticamente per un periodo di tempo, ad esempio utilizzando attività pianificate. L'esempio seguente illustra come aggiornare i limiti di velocità della larghezza di banda di un gateway usando AWS Tools for Windows PowerShell. Per utilizzare il codice di esempio, è necessario avere dimestichezza con l'esecuzione di uno script. PowerShell Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS Strumenti per PowerShell .

Example : Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS Tools for Windows PowerShell

Il seguente esempio di PowerShell script aggiorna i limiti di velocità di larghezza di banda di un gateway. Per utilizzare questo script di esempio, devi fornire il gateway Amazon Resource Name (ARN) e il limite di upload.

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule

    .NOTES
        PREREQUISITES:
        1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
        2) Credentials and region stored in session using Initialize-AWSDefault.
        For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html


    .EXAMPLE
        powershell.exe .\SG_UpdateBandwidth.ps1
    #>

    $UploadBandwidthRate = 100 * 1024 * 1024
```

```
   $gatewayARN = "*** provide gateway ARN ***"

   $bandwidthRateLimitInterval = New-Object
Amazon.StorageGateway.Model.BandwidthRateLimitInterval
   $bandwidthRateLimitInterval.StartHourOfDay = 0
   $bandwidthRateLimitInterval.StartMinuteOfHour = 0
   $bandwidthRateLimitInterval.EndHourOfDay = 23
   $bandwidthRateLimitInterval.EndMinuteOfHour = 59
   $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
   $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
$UploadBandwidthRate

   #Update Bandwidth Rate Limits
   Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                       -BandwidthRateLimitInterval
@($bandwidthRateLimitInterval)

   $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

   Write-Output("`nGateway: " + $gatewayARN);
   Write-Output("`nNew bandwidth throttle schedule: " +
$schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

Monitoraggio di Storage Gateway

Gli argomenti di questa sezione descrivono come monitorare un gateway utilizzando Amazon CloudWatch, incluso il monitoraggio dello storage della cache e di altre risorse associate al gateway. È possibile utilizzare la console Storage Gateway per visualizzare i parametri e gli allarmi per il gateway. Ad esempio, puoi visualizzare il numero di byte utilizzati nelle operazioni di lettura e scrittura, il tempo impiegato nelle operazioni di lettura e scrittura e il tempo impiegato per recuperare i dati dal cloud. AWS I parametri consentono di monitorare l'integrità del gateway e di impostare allarmi di notifica quando uno o più parametri sono al di fuori di una soglia definita.

Storage Gateway fornisce CloudWatch metriche senza costi aggiuntivi. I parametri Storage Gateway sono registrati per un periodo di due settimane. Utilizzando queste metriche, è possibile accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni dei gateway. Storage Gateway fornisce anche CloudWatch allarmi, ad eccezione degli allarmi ad alta risoluzione, senza costi aggiuntivi. Per ulteriori informazioni sui CloudWatch prezzi, consulta la pagina CloudWatch dei prezzi di Amazon. Per ulteriori informazioni CloudWatch, consulta la Amazon CloudWatch User Guide.

Argomenti

- CloudWatch Comprensione degli allarmi- Scopri le informazioni di base sugli CloudWatch allarmi, inclusi gli stati degli allarmi e le configurazioni consigliate.
- Crea allarmi consigliati CloudWatch - Scopri come configurare in modo rapido e automatico tutti gli CloudWatch allarmi consigliati come parte del processo di configurazione iniziale di File Gateway.
- Crea un CloudWatch allarme personalizzato- Scopri come creare un CloudWatch allarme personalizzato per monitorare una metrica specifica utilizzando criteri di valutazione specifici per attivare gli stati di allarme e inviare notifiche.
- - Scopri come visualizzare CloudWatch i log e i log di controllo e trova informazioni sullo specifico gateway e sulle metriche del file system di condivisione file riportate dal gateway.

CloudWatch Comprensione degli allarmi

CloudWatch gli allarmi monitorano le informazioni sul gateway in base a metriche ed espressioni. È possibile aggiungere CloudWatch allarmi per il gateway e visualizzarne lo stato nella console Storage Gateway. Per ogni allarme, si specificano le condizioni che attiveranno lo stato ALARM. Gli

indicatori di stato degli allarmi nella console Storage Gateway diventano rossi quando si trova nello stato ALLARME, semplificando il monitoraggio dello stato in modo proattivo. È possibile configurare gli allarmi per richiamare automaticamente le azioni in base a cambiamenti di stato sostenuti. Per ulteriori informazioni sugli CloudWatch allarmi, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

> **Note**
>
> Se non disponi dell'autorizzazione per la visualizzazione CloudWatch, non puoi visualizzare gli allarmi.

Per ogni gateway attivato, si consiglia di creare i seguenti allarmi CloudWatch:

- Attesa I/O elevata: `IoWaitpercent` >= 20 per 3 antidatato in 15 minuti
- Percentuale di cache dirty: `CachePercentDirty` > 80 per 4 datapoint entro 20 minuti
- File non caricati: `FilesFailingUpload` >= 1 per 1 datapoint entro 5 minuti
- Condivisioni di file non disponibili: `FileSharesUnavailable` >= 1 per 1 datapoint entro 5 minuti
- Notifiche Health: `HealthNotifications` >= 1 per 1 datapoint entro 5 minuti. Quando configuri questo allarme, imposta Trattamento dei dati mancanti su notBreaching.

  > **Note**
  >
  > È possibile impostare un avviso di notifica di stato solo se il gateway aveva una precedente notifica di stato in CloudWatch.

Per i gateway su piattaforme VMware host che fanno parte di un cluster VMware ad alta disponibilità, consigliamo anche questo allarme aggiuntivo: CloudWatch

- Notifiche di disponibilità: `AvailabilityNotifications` >= 1 per 1 datapoint entro 5 minuti. Quando configuri questo allarme, imposta Trattamento dei dati mancanti su notBreaching.

La tabella seguente descrive gli stati di allarme. CloudWatch

Stato	Description
OK	Il parametro o espressione rientra nella soglia definita.
Allarme	Il parametro o espressione non rientra nella soglia definita.
Dati insufficienti	L'allarme è stato appena attivato, il parametro non è disponibile o la quantità di dati non è sufficiente affinché il parametro determini lo stato dell'allarme.
Nessuno	Non vengono creati allarmi per il gateway. Per creare un nuovo avviso, vedere Crea un CloudWatch allarme personalizzato per il tuo gateway.
Non disponibile	Lo stato dell'allarme è sconosciuto. Scegliere Unavailable (Non disponibile) per visualizz are le informazioni sugli errori nella scheda Monitoring (Monitoraggio) .

Creazione di CloudWatch allarmi consigliati per il gateway

Quando si crea un nuovo gateway utilizzando la console Storage Gateway, è possibile scegliere di creare automaticamente tutti gli CloudWatch allarmi consigliati come parte del processo di configurazione iniziale. Per ulteriori informazioni, consulta Configurare Amazon S3 File Gateway Gateway. Se desideri aggiungere o aggiornare gli CloudWatch allarmi consigliati per un gateway esistente dopo aver già completato la prima configurazione, usa la seguente procedura.

Per aggiungere o aggiornare gli CloudWatch allarmi consigliati per un gateway esistente

> **Note**
>
> Questa funzionalità richiede le autorizzazioni relative alle CloudWatch policy, che non vengono concesse automaticamente come parte della policy di accesso completo

preconfigurata di Storage Gateway. Assicurati che la tua politica di sicurezza conceda le seguenti autorizzazioni prima di tentare di creare allarmi consigliati: CloudWatch

- `cloudwatch:PutMetricAlarm`: creazione di allarmi
- `cloudwatch:DisableAlarmActions`: disattivazione delle azioni di allarme
- `cloudwatch:EnableAlarmActions`: attivazione delle azioni di allarme
- `cloudwatch:DeleteAlarms`: eliminazione di allarmi

1. Aprire la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/.
2. Nel riquadro di navigazione sul lato sinistro della pagina, scegli Gateway, quindi scegli il gateway per il quale desideri creare gli allarmi consigliati CloudWatch .
3. Nella pagina Dettagli del gateway, scegli la scheda Monitoraggio.
4. In Allarmi, scegli Crea allarmi consigliati. Gli allarmi consigliati vengono creati automaticamente.

   La sezione Allarmi elenca tutti gli CloudWatch allarmi per un gateway specifico. Da qui, puoi selezionare ed eliminare uno o più allarmi, attivare o disattivare le azioni di allarme e creare nuovi allarmi.

Crea un CloudWatch allarme personalizzato per il tuo gateway

CloudWatch utilizza Amazon Simple Notification Service (Amazon SNS) per inviare notifiche di allarme quando un allarme cambia stato. Un allarme controlla un singolo parametro in un periodo di tempo specificato ed esegue una o più operazioni in base al valore del parametro relativo a una determinata soglia in una serie di periodi di tempo. L'operazione corrisponde all'invio di una notifica a un argomento Amazon SNS. Puoi creare un argomento Amazon SNS quando crei un CloudWatch allarme. Per ulteriori informazioni su Amazon SNS, consulta Che cos'è Amazon SNS? nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Per creare un CloudWatch allarme nella console Storage Gateway

1. Aprire la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/.
2. Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera creare un allarme.
3. Nella pagina dei dettagli del gateway, scegliere la scheda Monitoraggio.
4. In Allarmi, scegli Crea allarme per aprire la CloudWatch console.

5. Usa la CloudWatch console per creare il tipo di allarme che desideri. Puoi creare i seguenti tipi di allarmi:

   - Allarme di soglia statica: un allarme basato su una soglia impostata per un parametro scelto. L'allarme entra nello stato ALARM quando la metrica supera la soglia per un determinato numero di periodi di valutazione.

     Per creare un allarme con soglia statica, consulta Creazione di un CloudWatch allarme basato su una soglia statica nella Amazon CloudWatch User Guide.

   - Allarme di rilevamento delle anomalie: il rilevamento delle anomalie recupera i dati dei parametri nel tempo e crea un modello di valori previsti. Imposta un valore per la soglia di rilevamento delle anomalie e CloudWatch utilizza questa soglia con il modello per determinare l'intervallo di valori «normale» per la metrica. Un valore più alto per la soglia produce un intervallo più ampio di valori "normali". Puoi decidere se l'allarme viene attivato solo quando il valore del parametro è al di sopra dell'intervallo di valori previsti, solo se si trova al di sotto di tale intervallo oppure è sopra o sotto l'intervallo.

     Per creare un allarme di rilevamento delle anomalie, consulta Creazione di un CloudWatch allarme basato sul rilevamento delle anomalie nella Amazon CloudWatch User Guide.

   - Allarme di espressione matematica del parametro: un allarme basato su uno o più parametri utilizzati in un'espressione matematica. Si specificano l'espressione, la soglia e i periodi di valutazione.

     Per creare un allarme con espressione matematica metrica, consulta Creazione di un CloudWatch allarme basato su un'espressione matematica metrica nella Amazon User Guide. CloudWatch

   - Allarme composito: un allarme che determina il suo stato di allarme osservando gli stati di allarme di altri allarmi. Un allarme composito può aiutare a ridurre il rumore di allarme.

     Per creare un allarme composito, consulta Creazione di un allarme composito nella Amazon CloudWatch User Guide.

6. Dopo aver creato l'allarme nella CloudWatch console, tornare alla console Storage Gateway. È possibile visualizzare l'allarme effettuando una delle seguenti operazioni:

   - Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera visualizzare gli allarmi. Nella scheda Dettagli, in Allarmi, scegli CloudWatch Allarmi.

- Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera visualizzare gli allarmi e quindi scegliere la scheda Monitoraggio.

  La sezione Allarmi elenca tutti gli CloudWatch allarmi per un gateway specifico. Da qui, puoi selezionare ed eliminare uno o più allarmi, attivare o disattivare le azioni di allarme e creare nuovi allarmi.
- Nel pannello di navigazione scegliere Gateway, quindi scegliere lo stato di allarme del gateway per cui si desidera visualizzare gli allarmi.

Per informazioni su come modificare o eliminare un avviso, consulta Modificare o eliminare un avviso. CloudWatch

> **Note**
>
> Quando si elimina un gateway utilizzando la console Storage Gateway, vengono eliminati automaticamente anche tutti gli CloudWatch allarmi associati al gateway.

Puoi monitorare il tuo S3 File Gateway e le risorse associate Gateway di archiviazione AWS utilizzando i CloudWatch parametri e i log di controllo di Amazon. Puoi anche utilizzare CloudWatch Events per ricevere notifiche quando le operazioni sui file sono terminate.

Argomenti

- Ottenere i registri di integrità di S3 FSx File Gateway con CloudWatch gruppi di log
- Utilizzo dei CloudWatch parametri di Amazon
- Ricevere notifiche sulle operazioni sui file
- Comprendere i parametri del gateway
- Comprensione delle metriche relative alla condivisione dei file
-

Ottenere i registri di integrità di S3 FSx File Gateway con CloudWatch gruppi di log

Puoi utilizzare Amazon CloudWatch Logs per ottenere informazioni sullo stato di salute del tuo S3 File Gateway e delle risorse correlate. Puoi utilizzare i log per monitorare il gateway alla ricerca di

eventuali errori. Inoltre, puoi utilizzare i filtri di CloudWatch abbonamento Amazon per automatizzare l'elaborazione delle informazioni di registro in tempo reale. Per ulteriori informazioni, consulta Elaborazione in tempo reale dei dati di registro con abbonamenti nella Amazon CloudWatch User Guide.

Ad esempio, puoi configurare un gruppo di CloudWatch log per monitorare il gateway e ricevere una notifica quando il tuo S3 File Gateway non riesce a caricare file su un bucket Amazon S3. Puoi configurare il gruppo quando attivi il gateway o dopo che il gateway è stato attivato e funzionante. Per informazioni su come configurare un gruppo di CloudWatch log durante l'attivazione di un gateway, vedere. Configura il tuo Amazon S3 File Gateway Per informazioni generali sui gruppi di CloudWatch log, consulta Working with Log Groups and Log Streams nella Amazon CloudWatch User Guide.

Di seguito è riportato un esempio di errore segnalato da un S3 File Gateway.

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/amzn-s3-demo-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

Questo errore indica che S3 File Gateway non è in grado di caricare l'oggetto su Amazon S3 perché è passato dalla classe di storage Amazon S3 Standard `myFolder/myFile.text` alla classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Nel log dello stato del gateway precedente, questi elementi specificano le informazioni fornite:

- `source: share-E1A2B34C` indica la condivisione file che ha riscontrato questo errore.
- `"type": "InaccessibleStorageClass"` indica il tipo di errore che si è verificato. In questo caso, questo errore si è verificato quando il gateway stava tentando di caricare l'oggetto specificato su Amazon S3 o di leggerlo da Amazon S3. Tuttavia, in questo caso, l'oggetto è passato ad Amazon Glacier. Il valore di `"type"` può essere qualsiasi errore riscontrato da S3 File Gateway. Per un elenco dei possibili errori, consulta Risoluzione dei problemi: problemi relativi a File Gateway

- `"operation": "S3Upload"`indica che questo errore si è verificato quando il gateway stava tentando di caricare questo oggetto su S3.
- `"key": "myFolder/myFile.text"` indica l'oggetto che ha causato l'errore.
- `gateway": "sgw-B1D123D4`indica che S3 File Gateway ha riscontrato questo errore.
- `"timestamp": "1565740862516"`indica l'ora in cui si è verificato l'errore.

Per informazioni su come risolvere gli errori che possono essere segnalati da S3 File Gateway Gateway, vedere. Risoluzione dei problemi: problemi relativi a File Gateway

Configurazione di un gruppo di CloudWatch log dopo l'attivazione del gateway

La procedura seguente mostra come configurare un gruppo di CloudWatch log dopo l'attivazione del gateway.

Per configurare un gruppo di CloudWatch log in modo che funzioni con S3 File Gateway Gateway

1. Accedi Console di gestione AWS e apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway per cui desideri configurare il gruppo di CloudWatch log.
3. Per Azioni, scegli Modifica le informazioni sul gateway.
4. Per Scegli come configurare il gruppo di log, scegli una delle seguenti opzioni:

   - Crea un nuovo gruppo di log per creare un nuovo gruppo di CloudWatch log.
   - Utilizza un gruppo di log esistente per utilizzare un gruppo di CloudWatch log già esistente.

     Scegli un gruppo di log dall'elenco dei gruppi di log esistenti.
   - Disattiva la registrazione se non desideri monitorare il gateway utilizzando i gruppi di CloudWatch log.
5. Scegli Save changes (Salva modifiche).
6. Per visualizzare i log sullo stato del gateway, procedi come indicato di seguito:

   1. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway per cui hai configurato il gruppo di CloudWatch log.
   2. Scegli la scheda Dettagli e, in Health logs, scegli CloudWatchLogs. La pagina dei dettagli del gruppo di log si apre nella CloudWatch console.

Utilizzo dei CloudWatch parametri di Amazon

Puoi ottenere i dati di monitoraggio per il tuo S3 File Gateway FSx utilizzando Console di gestione AWS o l' CloudWatch API. La console mostra una serie di grafici basati sui dati grezzi dell' CloudWatch API. L' CloudWatch API può essere utilizzata anche tramite uno dei AWS SDKsnostri strumenti CloudWatch API di Amazon. In base alle tue esigenze, potresti decidere di utilizzare i grafici visualizzati nella console o quelli recuperati dall'API.

Indipendentemente dal metodo utilizzato per lavorare con le metriche, devi specificare le seguenti informazioni:

- Dimensione del parametro da usare. Una dimensione è una coppia nome-valore che consente di identificare una metrica in modo univoco. Le dimensioni di Storage Gateway sono `GatewayId` e `GatewayName`. Nella CloudWatch console, puoi utilizzare la `Gateway Metrics` vista per selezionare dimensioni specifiche del gateway. Per ulteriori informazioni sulle dimensioni, consulta Dimensions nella Amazon CloudWatch User Guide.
- Il nome del parametro, ad esempio `ReadBytes`.

La tabella seguente contiene un riepilogo dei tipi di dati dei parametri di Storage Gateway disponibili.

Spazio dei CloudWatch nomi Amazon	Dimensione	Description
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Queste dimensioni filtrano in base ai dati dei parametri che descrivono gli aspetti del gateway. Puoi identificare un S3 File Gateway con cui lavorare specificando sia le dimensioni che le `GatewayId` dimensioni. `GatewayName` I dati di throughput e latenza di un gateway si basano su tutte le condivisioni file nel gateway. I dati sono disponibili gratuitamente e automaticamente in intervalli di 5 minuti.

L'uso di parametri di gateway e file è simile all'uso di altri parametri del servizio. Puoi trovare una presentazione delle attività dei parametri più comuni nella documentazione di CloudWatch elencata di seguito:

- Visualizzazione delle metriche disponibili
- Ottenere statistiche per una metrica
- Creazione di allarmi CloudWatch

Ricevere notifiche sulle operazioni sui file

Storage Gateway può avviare i seguenti CloudWatch eventi al termine delle operazioni sui file:

- Puoi ricevere una notifica quando il gateway termina il caricamento asincrono dei tuoi file dalla condivisione di file su Amazon S3. Utilizza il `NotificationPolicy` parametro per richiedere una notifica di caricamento del file. In questo modo viene inviata una notifica per ogni caricamento di file completato su Amazon S3. Per ulteriori informazioni, consulta Ricevere una notifica di caricamento dei file.
- Puoi ricevere una notifica quando il gateway termina il caricamento asincrono del tuo set di file di lavoro dalla condivisione di file su Amazon S3. Utilizza l'operazione NotifyWhenUploadedAPI per richiedere una notifica di caricamento di un set di file funzionante. Questo invia una notifica quando tutti i file del set di file di lavoro sono stati caricati su Amazon S3. Per ulteriori informazioni, consulta Ricezione della notifica di caricamento di un set di file funzionante.
- È possibile ricevere una notifica quando il gateway termina l'aggiornamento della cache per il tuo bucket S3. Quando richiami l'RefreshCacheoperazione tramite la console o l'API di Storage Gateway, iscriviti alla notifica al termine dell'operazione. Per ulteriori informazioni, consulta Ricezione della notifica di aggiornamento della cache.

Al termine dell'operazione sui file richiesta, Storage Gateway invia una notifica tramite CloudWatch Eventi. Puoi configurare CloudWatch Events per inviare la notifica tramite destinazioni di eventi come Amazon SNS, Amazon SQS o una funzione. AWS Lambda Ad esempio, puoi configurare un target Amazon SNS per inviare la notifica ai consumatori di Amazon SNS, ad esempio un'e-mail o un messaggio di testo. Per informazioni sugli CloudWatch eventi, consulta What is CloudWatch Events?

Per impostare la notifica CloudWatch degli eventi

1. Crea un target, ad esempio un argomento Amazon SNS o una funzione Lambda, da richiamare quando si verifica l'evento richiesto in Storage Gateway.
2. Crea una regola nella console CloudWatch Eventi per richiamare le destinazioni in base a un evento in Storage Gateway.
3. Nella regola, crea un modello di evento per il tipo di evento. La notifica inviata quando l'evento corrisponde a questo schema di regole.
4. Selezionare la destinazione e configurare le impostazioni.

L'esempio seguente mostra una regola che avvia il tipo di evento specificato nel gateway specificato e nella AWS regione specificata. Ad esempio, è possibile specificare `Storage Gateway File Upload Event` come tipo di evento.

```
{
   "source":[
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

Per informazioni su come utilizzare le regole CloudWatch Events, consulta Creazione di una regola CloudWatch Events che si attiva su un evento nella Amazon CloudWatch Events User Guide.

Ricevere una notifica di caricamento dei file

Esistono due casi d'uso in cui è possibile utilizzare la notifica di caricamento dei file:

- Per automatizzare l'elaborazione nel cloud dei file caricati, puoi richiamare il `NotificationPolicy` parametro e ottenere un ID di notifica. La notifica che si verifica quando i file sono stati caricati ha lo stesso ID di notifica di quella restituita dall'API. Se mappate questo ID di notifica per tenere traccia dell'elenco dei file che state caricando, potete avviare l'elaborazione del file caricato AWS quando viene generato l'evento con lo stesso ID.

- Per i casi d'uso relativi alla distribuzione di contenuti, puoi avere due S3 File Gateway mappati allo stesso bucket Amazon S3. Il client di condivisione file per Gateway1 può caricare nuovi file su Amazon S3 e i file vengono letti dai client di condivisione file su Gateway2. I file vengono caricati su Amazon S3, ma non sono visibili su Gateway2 perché utilizza una versione dei file memorizzata nella cache locale di Amazon S3. Per rendere visibili i file in Gateway2, puoi utilizzare il `NotificationPolicy` parametro per richiedere una notifica di caricamento dei file a Gateway1 per avvisarti quando il caricamento del file è terminato. È quindi possibile utilizzare CloudWatch Events per inviare automaticamente una RefreshCacherichiesta di condivisione di file su Gateway2. Una volta completata la RefreshCacherichiesta, il nuovo file è visibile in Gateway2.

Example Esempio: notifica di caricamento di file

L'esempio seguente mostra una notifica di caricamento di file che viene inviata all'utente CloudWatch quando l'evento corrisponde alla regola creata. Questa notifica è in formato JSON. È possibile configurare questa notifica in modo che venga in forma di SMS. Il valore del campo `detail-type` è `Storage Gateway Object Upload Event`.

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "amzn-s3-demo-bucket",
    }
}
```

Nomi di campo	Description
versione	La versione corrente della policy IAM.
id	L'ID che identifica la policy IAM.
detail-type (tipo di dettaglio)	Una descrizione dell'evento che ha avviato la notifica inviata.
origine	Il AWS servizio che è l'origine della richiesta e della notifica.
account	L'ID dell' AWS account da cui sono state generate la richiesta e la notifica.
time	Quando è stata effettuata la richiesta di caricamento di file su Amazon S3.
region	La AWS regione da cui sono state inviate la richiesta e la notifica.
risorse	Le risorse Storage Gateway a cui si applica la policy.
dimensione dell'oggetto	La dimensione dell'oggetto in byte.
tempo di modifica	L'ora in cui il client ha modificato il file.
chiave-oggetto	Il percorso del file.
event-type	Gli CloudWatch eventi che hanno avviato la notifica.
prefisso	Il nome del prefisso del bucket S3.
bucket-name	Nome del bucket S3.

Ricezione della notifica di caricamento di un set di file funzionante

Esistono due casi d'uso in cui è possibile utilizzare la notifica di caricamento del set di file di lavoro:

- Per automatizzare l'elaborazione nel cloud dei file caricati, puoi chiamare l'`NotifyWhenUploaded`API e ottenere un ID di notifica. La notifica che si verifica quando il set di lavoro di file è stato caricato ha lo stesso ID di notifica di quello restituito dall'API. Se mappate questo ID di notifica per tenere traccia dell'elenco dei file che state caricando, potete avviare l'elaborazione del working set di file che vengono caricati AWS quando viene generato l'evento con lo stesso ID.
- Per i casi d'uso relativi alla distribuzione di contenuti, puoi avere due S3 File Gateway mappati allo stesso bucket Amazon S3. Il client di condivisione file per Gateway1 può caricare nuovi file su Amazon S3 e i file vengono letti dai client di condivisione file su Gateway2. I file vengono caricati su Amazon S3, ma non sono visibili su Gateway2 perché utilizza una versione dei file memorizzata nella cache locale in S3. Per rendere visibili i file in Gateway2, utilizza l'operazione NotifyWhenUploadedAPI per richiedere la notifica di caricamento dei file da Gateway1, per avvisarti quando il caricamento del set di file di lavoro è terminato. È quindi possibile utilizzare gli CloudWatch eventi per inviare automaticamente una RefreshCacherichiesta per la condivisione di file su Gateway2. Una volta completata la RefreshCacherichiesta, i nuovi file sono visibili in Gateway2. Questa operazione non importa i file nella memoria cache del gateway. Aggiorna solo l'inventario memorizzato nella cache per riflettere le modifiche nell'inventario degli oggetti nel bucket S3.

Example Esempio: notifica di caricamento di un set di file funzionanti

L'esempio seguente mostra una notifica di caricamento del set di file di lavoro che viene inviata all'utente CloudWatch quando l'evento corrisponde alla regola creata. Questa notifica è in formato JSON. È possibile configurare questa notifica in modo che venga in forma di SMS. Il valore del campo `detail-type` è `Storage Gateway File Upload Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway File Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
```

```
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

Nomi di campo	Description
versione	La versione corrente della policy IAM.
id	L'ID che identifica la policy IAM.
detail-type (tipo di dettaglio)	Una descrizione dell'evento che ha avviato la notifica inviata.
origine	Il AWS servizio che è l'origine della richiesta e della notifica.
account	L'ID dell' AWS account da cui sono state generate la richiesta e la notifica.
time	Quando è stata effettuata la richiesta di caricamento di file su Amazon S3.
region	La AWS regione da cui sono state inviate la richiesta e la notifica.
risorse	Le risorse Storage Gateway a cui si applica la policy.
event-type	Gli CloudWatch eventi che hanno avviato la notifica.
notification-id	L'ID generato in modo casuale della notifica che è stata inviata. Questo ID è nel formato UUID. Questo è l'ID della notifica che viene restituito quando `NotifyWhenUploaded` viene chiamato.

Nomi di campo	Description
richiesta-ricevuta	Quando il gateway ha ricevuto la richiesta `NotifyWhenUploaded` .
completed	Quando tutti i file del working-set sono stati caricati su Amazon S3.

Ricezione della notifica di aggiornamento della cache

Per il caso d'uso della notifica di aggiornamento della cache, puoi avere due S3 File Gateway mappati allo stesso bucket Amazon S3 e il client NFS per Gateway1 carica nuovi file nel bucket S3. I file vengono caricati su Amazon S3, ma non vengono visualizzati in Gateway2 finché non aggiorni la cache. Questo perché Gateway2 utilizza una versione memorizzata nella cache locale dei file in Amazon S3. È possibile eseguire un'operazione con i file nel Gateway2 quando l'aggiornamento della cache è terminato. La visualizzazione di file di grandi dimensioni potrebbe richiedere del tempo in Gateway2, quindi potresti voler ricevere una notifica quando viene completato l'aggiornamento della cache. È possibile richiedere la notifica di aggiornamento della cache dal Gateway2 per sapere quando tutti i file sono visibili in Gateway2.

Example Esempio: notifica di aggiornamento della cache

L'esempio seguente mostra una notifica di aggiornamento della cache che viene inviata all'utente CloudWatch quando l'evento corrisponde alla regola creata. Questa notifica è in formato JSON. È possibile configurare questa notifica in modo che venga in forma di SMS. Il valore del campo `detail-type` è `Storage Gateway Refresh Cache Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
```

```
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

Nomi di campo	Description
versione	La versione corrente della policy IAM.
id	L'ID che identifica la policy IAM.
detail-type (tipo di dettaglio)	Una descrizione del tipo di evento che ha avviato la notifica inviata.
origine	Il AWS servizio che è l'origine della richiesta e della notifica.
account	L'ID dell' AWS account da cui sono state generate la richiesta e la notifica.
time	Quando è stata effettuata la richiesta per aggiornare i file nel set di lavoro.
region	La AWS regione da cui sono state inviate la richiesta e la notifica.
risorse	Le risorse Storage Gateway a cui si applica la policy.
event-type	Gli CloudWatch eventi che hanno avviato la notifica.
notification-id	L'ID generato in modo casuale della notifica che è stata inviata. Questo ID è nel formato UUID. Questo è l'ID della notifica che viene

Nomi di campo	Description
	restituito quando `RefreshCache` viene chiamato.
tutorial	quando il gateway ha ricevuto la `RefreshCache` richiesta e l'aggiornamento è stato avviato.
completed	Quando l'aggiornamento del set di lavoro è stato completato.
folderList	Un elenco separato da virgole dei percorsi di cartelle che sono stati aggiornati nella cache. Il valore predefinito è ["/"].

Comprendere i parametri del gateway

La tabella seguente descrive le metriche che riguardano S3 File Gateway. A ogni gateway è associata una serie di metriche. Alcune metriche specifiche del gateway hanno lo stesso nome di alcune metriche. file-share-specific Queste metriche rappresentano gli stessi tipi di misurazioni, ma si riferiscono al gateway anziché alla condivisione di file.

Specificate sempre se desiderate lavorare con un gateway o una condivisione di file quando lavorate con una metrica particolare. In particolare, quando si lavora con le metriche del gateway, è necessario specificare le metriche `Gateway Name` per il gateway di cui si desidera visualizzare i dati metrici. Per ulteriori informazioni, consulta Utilizzo dei CloudWatch parametri di Amazon.

> **Note**
>
> Alcuni parametri restituiscono punti dati solo quando sono stati generati nuovi dati durante il periodo di monitoraggio più recente.

Metrica	Description
`AuditNotifications`	Questa metrica riporta il numero di log di controllo emessi. Unità: numero
`AvailabilityNotifications`	Questa metrica riporta il numero di notifiche sanitarie relative alla disponibilità generate dal gateway nel periodo di riferimento. Unità: numero
`CacheFileSize`	Questa metrica tiene traccia della dimensione dei file nella cache del gateway. Utilizza questa metrica con la `Average` statistic a per misurare la dimensione media di un file nella cache del gateway. Utilizza questa metrica con la `Max` statistica per misurare la dimensione massima di un file nella cache del gateway. Unità: byte
`CacheFree`	Questa metrica riporta il numero di byte disponibili nella cache del gateway. Unità: byte
`CacheHitPercent`	Percentuale di operazioni di lettura delle applicazioni dal gateway servite dalla cache. Il campione si riferisce al termine del periodo di reporting. Quando non ci sono operazioni di lettura delle applicazioni dal gateway, questa metrica riporta il 100%.

Metrica	Description
	Unità: percentuale
`CachePercentDirty`	La percentuale complessiva della cache del gateway che non è stata mantenuta in modo persistente. AWS Il campione si riferisce al termine del periodo di reporting. Utilizza questa metrica con la `Sum` statistica. Idealmente, questa metrica dovrebbe rimanere bassa. Unità: percentuale
`CachePercentUsed`	La percentuale di cache di dati utilizzata nell'intero gateway. Il campione si riferisce al termine del periodo di reporting. Unità: percentuale
`CacheUsed`	Questa metrica riporta il numero di byte utilizzat i nella cache del gateway. Unità: byte
`CloudBytesDownloaded`	Il numero totale di byte da cui il gateway è stato scaricato AWS durante il periodo di riferimento. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

Metrica	Description
`CloudBytesUploaded`	Il numero totale di byte in cui il gateway è stato caricato AWS durante il periodo di riferimento. Utilizza questa metrica con la `Sum` statistica per misurare la velocità effettiva e con la `Samples` statistica per misurare le input/output operazion i al secondo (IOPS). Unità: byte
`FilesFailingUpload`	Questa metrica tiene traccia del numero di file su cui non viene eseguito il caricamento. AWS Questi file genereranno notifiche sanitarie che contengono ulteriori informazioni sul problema. Utilizza questa metrica con la `Sum` statistica per mostrare il numero di file su cui attualmente non è possibile caricare. AWS Unità: numero
`FileSharesUnavailable`	Questa metrica fornisce il numero di condivisi oni di file su questi gateway che si trovano nello stato Non disponibile. Se questa metrica riporta che le condivisioni di file non sono disponibili, è probabile che vi sia un problema con il gateway che potrebbe causare un'interruzione del flusso di lavoro. Si consiglia di creare un allarme quando questa metrica riporta un valore diverso da zero. Unità: numero

Metrica	Description
FilesRenamed	Questa metrica tiene traccia del numero di file rinominati nel periodo di riferimento. Unità: numero
HealthNotifications	Questa metrica riporta il numero di notifiche sanitarie generate da questo gateway nel periodo di riferimento. Unità: numero
IndexEvictions	Questa metrica riporta il numero di file i cui metadati sono stati rimossi dall'indice dei metadati dei file memorizzato nella cache per fare spazio a nuove voci. Il gateway mantiene questo indice di metadati, che viene compilato dal Cloud on demand. AWS Unità: numero
IndexFetches	Questa metrica riporta il numero di file per i quali sono stati recuperati i metadati. Il gateway mantiene un indice memorizzato nella cache dei metadati dei file, che viene compilato dal Cloud su richiesta. AWS Unità: numero
IoWaitPercent	Questa metrica riporta la percentuale di tempo in cui la CPU è in attesa di una risposta dal disco locale. Unità: percentuale
MemTotalBytes	Questa metrica riporta la quantità totale di memoria sul gateway. Unità: byte

Metrica	Description
`MemUsedBytes`	Questa metrica riporta la quantità di memoria utilizzata sul gateway. Unità: byte
`NfsSessions`	Questa metrica riporta il numero di sessioni NFS attive sul gateway. Unità: numero
`RootDiskFreeBytes`	Questa metrica riporta il numero di byte disponibili sul disco principale del gateway. Se questa metrica riporta che meno di 20 GB sono gratuiti, è necessario aumentare la dimensione del disco principale. Per aumentare la dimensione del disco root, è possibile aumentare la dimensione del disco root esistente sulla macchina virtuale. Quando la macchina virtuale viene riavviata, il gateway riconosce l'aumento delle dimensioni sul disco principale. Unità: byte
`S3GetObjectRequestTime`	Questa metrica riporta il tempo impiegato dal gateway per completare le richieste S3 get Object. Unità: millisecondi
`S3PutObjectRequestTime`	Questa metrica riporta il tempo impiegato dal gateway per completare le richieste di oggetti put di S3. Unità: millisecondi

Metrica	Description
S3UploadPartRequestTime	Questa metrica riporta il tempo impiegato dal gateway per completare le richieste di caricamento delle parti di S3. Unità: millisecondi
SmbV1Sessions	Questa metrica riporta il numero di SMBv1 sessioni attive sul gateway. Unità: numero
SmbV2Sessions	Questa metrica riporta il numero di SMBv2 sessioni attive sul gateway. Unità: numero
SmbV3Sessions	Questa metrica riporta il numero di SMBv3 sessioni attive sul gateway. Unità: numero
TotalCacheSize	Questa metrica riporta la dimensione totale della cache. Unità: byte
UserCpuPercent	Questa metrica riporta la percentuale di tempo dedicata all'elaborazione del gateway. Unità: percentuale

Comprensione delle metriche relative alla condivisione dei file

Di seguito sono riportate le informazioni sulle metriche di Storage Gateway relative alle condivisioni di file. Ogni condivisione file dispone di un set di parametri a essa associati. Alcuni parametri specifici della condivisione file hanno lo stesso nome di alcuni parametri specifici del gateway. Questi parametri rappresentano lo stesso tipo di misure, ma vengono definiti per la condivisione file.

Specificare sempre se si desidera utilizzare un gateway o un parametro di condivisione dei file prima di utilizzare un parametro. Nello specifico, quando si lavora con i parametri di condivisione file, è necessario specificare `File share ID` che identifica il file per il quale si desidera visualizzare i parametri. Per ulteriori informazioni, consulta Utilizzo dei CloudWatch parametri di Amazon.

> **Note**
>
> Alcuni parametri restituiscono punti dati solo quando sono stati generati nuovi dati durante il periodo di monitoraggio più recente.

La tabella seguente descrive le metriche di Storage Gateway che è possibile utilizzare per ottenere informazioni sulle condivisioni di file.

Metrica	Description
`CacheHitPercent`	Percentuale di operazioni di lettura delle applicazioni dalle condivisioni di file servite dalla cache. Il campione si riferisce al termine del periodo di reporting. Quando non ci sono operazioni di lettura delle applicazioni dalla condivisione di file, questa metrica riporta il 100%. Unità: percentuale
`CachePercentDirty`	Il contributo della condivisione di file alla percentuale complessiva della cache del gateway che non è stata mantenuta in modo persistente. AWS Il campione si riferisce al termine del periodo di reporting. Utilizza questa metrica con la `Sum` statistica. Idealmente, questa metrica dovrebbe rimanere bassa.

Metrica	Description
	Note Utilizza la `CachePercentDirty` metrica del gateway per visualizzare la percentuale complessiva della cache del gateway che non è stata salvata in modo persistente. AWS Unità: percentuale
`CachePercentUsed`	La percentuale di cache di dati utilizzata nell'intero gateway. Il campione si riferisce al termine del periodo di reporting. Questa metrica specifica per la condivisione di file riporta lo stesso valore della metrica specifica del gateway corrispondente. Unità: percentuale
`CloudBytesUploaded`	Il numero totale di byte in cui il gateway è stato caricato durante il periodo di riferimento. AWS Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

Metrica	Description
`CloudBytesDownloaded`	Il numero totale di byte da cui il gateway è stato scaricato AWS durante il periodo di riferimento. Utilizzate questa metrica con la `Sum` statistic a per misurare la velocità effettiva e con la `Samples` statistica per misurare le input/output operazioni al secondo (IOPS). Unità: byte
`FilesFailingUpload`	Questa metrica tiene traccia del numero di file su cui non viene eseguito il caricamento. AWS Questi file genereranno notifiche sanitarie che contengono ulteriori informazioni sul problema. Utilizza questa metrica con la `Sum` statistica per mostrare il numero di file su cui attualmente non è possibile caricare. AWS Unità: numero
`ReadBytes`	Numero totale di byte letti dalle applicazioni on-premise durante il periodo di reporting per una condivisione file. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

Metrica	Description
`WriteBytes`	Numero totale di byte scritti nelle applicazioni in locale durante il periodo di reporting. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

I log di controllo di Amazon S3 File Gateway (S3 File Gateway) forniscono dettagli sull'accesso degli utenti a file e cartelle all'interno di una condivisione di file. Puoi utilizzarli per monitorare le attività degli utenti e agire se vengono identificati modelli di attività inappropriati.

Operazioni

La tabella seguente descrive le operazioni di accesso ai file di registro di controllo di S3 FSx File Gateway.

Nome operazione	Definizione
Leggere i dati	Leggi il contenuto di un file.
Scrivere i dati	Modifica il contenuto di un file.
Crea	Creare un nuovo file o una cartella.
Assegnazione di un nuovo nome	Rinominare un file o una cartella esistente.
Elimina	Eliminare un file o una cartella.
Attributi di scrittura	Aggiorna i metadati di file o cartelle (propriet arioACLs, gruppo, autorizzazioni).

Attributes

La tabella seguente descrive gli attributi di accesso ai file di registro di controllo di S3 File Gateway.

Attributo	Definizione
`accessMode`	L'impostazione di autorizzazione per l'oggetto.
`accountDomain` (Solo SMB)	Il dominio Active Directory (AD) a cui appartien e l'account client.
`accountName` (Solo SMB)	Il nome utente Active Directory del client.
`bucket`	Il nome del bucket S3.
`clientGid` (Solo NFS)	L'identificatore del gruppo dell'utente che accede all'oggetto.
`clientUid` (Solo NFS)	L'identificatore dell'utente che accede all'ogget to.
`ctime`	L'ora in cui il contenuto o i metadati dell'oggetto sono stati modificato, impostata dal client.
`groupId`	L'identificatore del gruppo proprietario dell'ogge tto.
`fileSizeInBytes`	La dimensione del file in byte, impostata dal client al momento della creazione del file.
`gateway`	L'ID gateway di storage.
`mtime`	Ora in cui il contenuto dell'oggetto è stato modificato, impostata dal client.
`newObjectName`	Il percorso completo del nuovo oggetto dopo che è stato rinominato.
`objectName`	Il percorso completo dell'oggetto.
`objectType`	Definisce se l'oggetto è un file o una cartella.
`operation`	Il nome dell'operazione di accesso dell'oggetto.

Attributo	Definizione
`ownerId`	L'identificatore per il proprietario dell'oggetto.
`securityDescriptor` (Solo SMB)	Visualizza l'elenco di controllo di accesso discrezionale (DACL) impostato su un oggetto, in formato SDDL.
`shareName`	Il nome della condivisione a cui si accede.
`source`	L'ID della condivisione file sottoposta ad audit.
`sourceAddress`	L'indirizzo IP del computer client di condivisione file.
`status`	Stato dell'operazione. Viene registrato solo l'esito positivo (gli errori vengono registrati ad eccezione degli errori derivanti da autorizza zioni negate).
`timestamp`	L'ora in cui si è verificata l'operazione in base al timestamp del sistema operativo del gateway.
`version`	Versione del formato del log di audit.

Attributi registrati per operazione

La tabella seguente descrive gli attributi del registro di controllo di S3 File Gateway registrati in ogni operazione di accesso ai file.

	Leggi i dati	Scrivi dati	Crea cartella	Crea un file	Rinomina file/ cartella	Eliminare file/ cartella	Attributi di scrittura (modifica solo ACL - SMB)	Attributi di scrittura (mostrati)	Scrivi attributi (chmod)	Scrivi attributi (chgrp)
access e			X	X					X	
accoun main (S SMB)	X	X	X	X	X	X	X	X	X	X
accoun me (Sol SMB)	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (solo NFS)	X	X	X	X	X	X		X	X	X
client (Solo NFS)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			X	X						
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						

	Leggi i dati	Scrivi dati	Crea cartella	Crea un file	Rinomina file/ cartella	Eliminare file/ cartella	Attributi di scrittura (modifica solo ACL - SMB)	Attributi di scrittura (mostrati)	Scrivi attributi (chmod)	Scrivi attributi (chgrp)
newObjName					X					
objecte	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securiescrip (Solo SMB)							X	X		
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
sourceress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timest	X	X	X	X	X	X	X	X	X	X

	Leggi i dati	Scrivi dati	Crea cartella	Crea un file	Rinomina file/ cartella	Eliminare file/ cartella	Attributi di scrittura (modifica solo ACL - SMB)	Attributi di scrittura (mostrati)	Scrivi attributi (chmod)	Scrivi attributi (chgrp)
`versic`	X	X	X	X	X	X	X	X	X	X

Crea un rapporto sulla cache per il tuo S3 File Gateway

S3 File Gateway può generare un report dei metadati per i file attualmente presenti nella cache di caricamento locale per una condivisione di file specifica. È possibile applicare filtri e criteri aggiuntivi che determinano quali tipi specifici di file memorizzati nella cache vengono visualizzati nel rapporto. È possibile utilizzare questo rapporto per identificare e risolvere i problemi relativi al gateway. Ad esempio, se hai file che non vengono caricati dal tuo gateway su Amazon S3, puoi generare un report che elenca i file specifici che non vengono caricati e i motivi dell'errore di caricamento. Il report è un file CSV contenente un elenco di file che corrispondono al set di parametri di filtro specificati. Il file di output viene archiviato come oggetto Amazon S3 in una posizione del bucket specificata durante la configurazione del report. Per creare un rapporto sulla cache utilizzando l' Gateway di archiviazione AWS API, vedere StartCacheReportlo Storage Gateway API Reference. Per creare un report sulla cache nella console Storage Gateway, utilizzare la procedura seguente.

Prerequisiti

- Il gateway deve disporre delle autorizzazioni `s3:PutObject` e `s3:AbortMultipartUpload` delle autorizzazioni per il bucket Amazon S3 in cui desideri archiviare il rapporto sulla cache.
- Al momento non possono essere in corso altri report sulla cache per la condivisione di file.
- Devono esserci meno di 10 report sulla cache esistenti per la condivisione di file.
- Il gateway deve essere online e connesso a AWS.
- Il disco principale del gateway deve avere almeno 20 GB di spazio libero.

Per creare un rapporto sulla cache utilizzando la console Storage Gateway

1. Aprire la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/.

2. Nel riquadro di navigazione sul lato sinistro della pagina, scegli Condivisioni di file, quindi scegli la condivisione di file per la quale desideri creare un rapporto sulla cache.
3. Dal menu a discesa Azioni, scegli Crea rapporto sulla cache.
4. Per la posizione Amazon S3, inserisci il bucket Amazon S3 e il prefisso della posizione in cui desideri salvare l'oggetto del file CSV del rapporto sulla cache completato in Amazon S3. Per selezionare il bucket e il prefisso dallo storage Amazon S3 esistente, scegli Browse S3.
5. Per il ruolo IAM, esegui una delle seguenti operazioni per specificare un ruolo IAM che conceda a File Gateway le autorizzazioni per generare e archiviare il rapporto sulla cache:

   - Per specificare un ruolo IAM esistente, scegli un ruolo dall'elenco a discesa.
   - Per creare manualmente un nuovo ruolo IAM, scegli Crea un ruolo, quindi crea il nuovo ruolo utilizzando la console IAM.

   > **Note**
   >
   > Il ruolo IAM specificato deve disporre delle seguenti autorizzazioni per scrivere oggetti nella posizione Amazon S3 del bucket di report e interrompere i caricamenti in più parti nel bucket di report:
   >
   > - `s3:PutObject`
   > - `s3:AbortMultipartUpload`
   >
   > Il ruolo deve inoltre consentire al `storagegateway.amazonaws.com` servizio di assumere il ruolo utilizzando l'`sts:AssumeRole`azione.

6. Per il filtro Report, effettuate una delle seguenti operazioni per determinare quali file verranno inclusi nel report della cache:

   - Per includere tutti i file memorizzati nella cache che al momento non vengono caricati su Amazon S3, scegli Tutti i file che non vengono caricati.
   - Per includere solo i file che non vengono caricati su Amazon S3 per un motivo specifico, scegli Solo motivi di errore di caricamento specifici. Quindi, per motivi di errore, seleziona uno o più dei seguenti motivi:
     - Classe di storage inaccessibile: il gateway non può accedere alla classe di storage Amazon S3 in cui è archiviato l'oggetto. Per ulteriori informazioni, consulta Error:. InaccessibleStorageClass

- Stato dell'oggetto non valido: lo stato del file sul gateway non corrisponde allo stato in Amazon S3. Per ulteriori informazioni, consulta Error:. InvalidObjectState
- Oggetto mancante: l'oggetto è stato eliminato o spostato in Amazon S3. Per ulteriori informazioni, consulta Error: ObjectMissing.
- Accesso negato a S3: il ruolo IAM di accesso al bucket Amazon S3 non consente al gateway di eseguire l'operazione di caricamento. Per ulteriori informazioni, consulta Error: S3. AccessDenied

> **Note**
>
> Il flag Files Failing Upload viene reimpostato ogni 24 ore e durante il riavvio del gateway. Se questo rapporto registra i file dopo il ripristino, ma prima che vengano nuovamente contrassegnati, non verranno segnalati come File non caricati.

7. Per utilizzare un endpoint VPC per connettersi a S3? , esegui una delle seguenti operazioni per specificare in che modo il gateway si connetterà al bucket Amazon S3:

   - Per connetterti direttamente senza usare Amazon VPC, scegli Connetti direttamente al bucket.
   - Per sfogliare un elenco di endpoint Amazon VPC esistenti, scegli Scegli un endpoint VPC, quindi specifica un endpoint dall'elenco a discesa degli endpoint VPC che appare.
   - Per specificare un endpoint Amazon VPC esistente in base al relativo nome DNS, scegli Inserisci un nome DNS dell'endpoint VPC, quindi inserisci il nome DNS nel campo Nome DNS dell'endpoint VPC che appare.

   > **Note**
   >
   > Se la condivisione di file utilizza un endpoint VPC per connettersi ad Amazon S3 per le normali operazioni, ti consigliamo di utilizzare lo stesso VPC quando configuri il rapporto sulla cache. La creazione di report sulla cache non riuscirà se il gateway non riesce a connettersi al bucket Amazon S3 per qualsiasi motivo, inclusa una configurazione VPC non valida.

8. (Facoltativo) In Tag: opzionale, scegli Aggiungi nuovo tag, quindi inserisci una chiave e un valore per il rapporto sulla cache.

Un tag è una coppia chiave-valore con distinzione tra maiuscole e minuscole che consente di classificare le risorse dello Storage Gateway. L'aggiunta di tag può semplificare il filtraggio e la ricerca del report della cache. Puoi ripetere questo passaggio per aggiungere fino a 50 tag.

9. Al termine, scegli Crea rapporto.

   Storage Gateway inizia a generare il report. È possibile controllare l'avanzamento e visualizzare lo stato nella scheda Cache reports della pagina dei dettagli relativa alla condivisione di file.

Visualizza e gestisci i report sulla cache per il tuo S3 File Gateway

I report sulla cache elencano i file attualmente presenti nella cache locale per una condivisione di file specifica, in base ai filtri e ai criteri specificati. È possibile visualizzare un elenco di report sulla cache esistenti per una condivisione di file specifica, controllare l'avanzamento e lo stato dei report ed eliminare i report non più necessari utilizzando l' Gateway di archiviazione AWS API o la console Storage Gateway.

Per gestire i report sulla cache utilizzando l'API, vedere le seguenti sezioni nello Storage Gateway API Reference:

- ListCacheReports
- DescribeCacheReport
- CancelCacheReport
- DeleteCacheReport

Per gestire i report della cache nella console Storage Gateway, utilizzare la procedura seguente.

Per gestire i report sulla cache utilizzando la console Storage Gateway

1. Aprire la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/.
2. Nel riquadro di navigazione sul lato sinistro della pagina, scegli Condivisioni di file, quindi scegli la condivisione di file per la quale desideri gestire i report della cache.
3. Nella pagina Dettagli per la condivisione di file, scegli la scheda Rapporti cache. Questa scheda elenca i report della cache esistenti per la condivisione di file e fornisce informazioni sullo stato, l'avanzamento e il percorso dell'oggetto in cui il file di report è archiviato in Amazon S3.
4. Esegui una delle seguenti operazioni:

- Per visualizzare dettagli aggiuntivi per un rapporto specifico, ad esempio l'ARN del rapporto e i tag associati, scegli un rapporto dalla colonna ID rapporto.
- Per specificare più report da gestire contemporaneamente, seleziona i report utilizzando la colonna della casella di controllo.

5. Per gestire uno o più report, scegli una delle seguenti opzioni dal menu a discesa Azioni:

   - Elimina rapporto cache: elimina il record del rapporto sulla cache dal database Storage Gateway. Elimina i record relativi ai report obsoleti della cache per fare spazio a nuovi report. Ogni condivisione di file può contenere fino a 10 report sulla cache esistenti in qualsiasi momento.

     > **Note**
     >
     > L'eliminazione del record del report della cache utilizzando questa procedura non elimina l'oggetto del file di report da Amazon S3.

   - Annulla rapporto: annulla un report attualmente in corso. Annulla un rapporto in corso se hai commesso un errore durante la configurazione del rapporto o se il completamento del rapporto impiega un tempo insolitamente lungo. Conferma l'annullamento quando richiesto.

     > **Note**
     >
     > I tempi di completamento possono variare in modo significativo a seconda del numero di file nella cache. In genere, la maggior parte dei report viene completata entro 5 minuti.

   La console Storage Gateway visualizza un messaggio che indica il risultato dell'azione di annullamento o eliminazione.

Comprensione delle informazioni fornite nei report sulla cache di S3 File Gateway

I report sulla cache elencano i file attualmente presenti nella cache locale per una condivisione di file specifica, in base ai filtri e ai criteri specificati. Ogni rapporto sulla cache include le seguenti informazioni:

- Bucket: il bucket o Access Point Amazon S3 associato alla condivisione di file.
- S3 ObjectKey: l'oggetto Amazon S3 che archivia i dati e i metadati per questo file. Questo oggetto contiene i dati più recenti che sono stati caricati su S3, ma potrebbero mancare dati che non vengono caricati su S3.
- FilePath— Il percorso del file per l'immissione del file nella cache del gateway. Qui è possibile trovare il file durante il montaggio e la navigazione nella condivisione di file.
- RenamedTo— Il nuovo percorso di un file rinominato. Quando si rinomina un file nella condivisione di file, il gateway deve tenere traccia sia della vecchia che della nuova posizione del file. Questo campo mostra dove è stato spostato il file e consente di tenere traccia delle operazioni di ridenominazione dei file, anche se un file è stato rinominato più volte. Queste informazioni sono particolarmente utili quando devi capire in che modo i file nella tua condivisione di file corrispondono agli oggetti nel tuo bucket Amazon S3.

  L'esempio seguente mostra le voci del report della cache per uno scenario complesso che prevede la sovrascrittura diretta di un file in Amazon S3 e la ridenominazione tramite File Gateway. In questo scenario, il gateway carica il file `A.txt` su S3, quindi rimuove il contenuto del file per liberare spazio nella cache locale. L'oggetto S3 associato viene quindi sovrascritto direttamente in S3, non tramite un'azione intrapresa dal gateway, il che provoca una mancata corrispondenza tra l'oggetto S3 e `InvalidObjectState` ciò che il gateway si aspetta. Allo stesso tempo, il file è stato rinominato tramite il gateway. `A.txt` `B.txt`

Bucket	S3 ObjectK	FilePat	Renam	Tipo	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplo	Upload or	SizeInB es	IsWholeFi leInCache
bucket- iad di esempi	A.txt	/B.txt		FILE	TRUE	FALSE	FALSE	TRUE	Invalid(jectSta	4	FALSE
bucket- iad di esempi	A.txt	/A.txt	/B.txt	FILE	TRUE	FALSE	TRUE	FALSE		4	FALSE

- Tipo: indica se la voce è per un `FILE` o. `DIRECTORY`
- IsDirty— Segnala `TRUE` eventuali modifiche al file che non sono state caricate su Amazon S3. Ciò include le modifiche ai metadati come il nome del file e read/write le autorizzazioni, anche se i dati del file non sono cambiati.

- IsDataDirty— Segnala TRUE se ci sono modifiche ai dati del file che non sono stati caricati su Amazon S3.
- IsDeleted— Segnala TRUE se il file è stato eliminato sul gateway. Se un file viene contrassegnato come eliminato, verrà sempre contrassegnato come sporco.
- IsFailingToUpload— Segnala TRUE se c'è un problema durante il caricamento del file su Amazon S3. Questo stato viene ripristinato ogni 24 ore per consentire al gateway di riprovare il caricamento e verificare se il problema è stato risolto. Il gateway rifiuta qualsiasi nuova operazione di scrittura per un file che non riesce a caricare. Se il gateway non ha l'intero file nella cache, rifiuta anche le operazioni di lettura.
- UploadError— L'errore che impedisce il caricamento del file su Amazon S3. Per ulteriori informazioni e per i passaggi consigliati per risolvere questi errori, consulta Risoluzione dei problemi relativi a File Gateway.
- SizeInBytes— La dimensione totale del file.
- IsWholeFileInCache— Indica TRUE se tutti i dati del file sono attualmente archiviati nella cache del gateway. Se questo è VERO per un file che non riesce a caricare su Amazon S3, il gateway consentirà la lettura del file.

Manutenzione del gateway

Manutenzione di Amazon S3 File Gateway implica la manutenzione generale per ottimizzare le prestazioni del gateway. Queste attività sono comuni a tutti i tipi di gateway.

Questa sezione contiene i seguenti argomenti, che descrivono concetti e procedure relativi alla manutenzione di S3 File Gateway:

Argomenti

- Gestione degli aggiornamenti del gateway— Scopri come attivare o disattivare gli aggiornamenti di manutenzione e modificare la pianificazione della finestra di manutenzione per File Gateway.
- Esecuzione delle attività di manutenzione utilizzando la console locale— Scopri come eseguire le attività di manutenzione utilizzando la console locale del gateway.
- Spegnimento della macchina virtuale gateway— Scopri cosa fare se devi spegnere o riavviare la macchina virtuale gateway per motivi di manutenzione, ad esempio quando applichi una patch all'hypervisor.
- Sostituzione del tuo S3 File Gateway esistente con una nuova istanza— Scopri come sostituire S3 File Gateway con una nuova istanza quando desideri migliorare le prestazioni o rispondere a una notifica di migrazione del gateway.
- Eliminazione del gateway e rimozione delle risorse associate— Scopri come eliminare il gateway utilizzando la Gateway di archiviazione AWS console e ripulire le risorse associate per evitare che ti venga addebitato alcun costo per il loro uso continuato.

Gestione degli aggiornamenti del gateway

Storage Gateway è costituito da un componente di servizi cloud gestiti e da un componente di appliance gateway che puoi distribuire in locale o su un' EC2 istanza Amazon nel cloud. AWS Entrambi i componenti ricevono aggiornamenti regolari. Gli argomenti di questa sezione descrivono la frequenza di questi aggiornamenti, il modo in cui vengono applicati e come configurare le impostazioni relative agli aggiornamenti sui gateway della distribuzione.

> **Important**
>
> È necessario trattare l'appliance Storage Gateway come una macchina virtuale gestita e non tentare di accedere o modificare l'installazione o il contenuto in alcun modo. Il

tentativo di installare o aggiornare qualsiasi pacchetto software utilizzando metodi diversi dal normale meccanismo di aggiornamento del AWS gateway (ad esempio, SSM o strumenti dell'hypervisor) potrebbe causare il malfunzionamento del gateway.
Storage Gateway aggiorna automaticamente e regolarmente l'appliance per mantenere sicurezza e stabilità. Le appliance Storage Gateway utilizzano Amazon Linux come sistema operativo di base. Puoi controllare lo stato dei problemi CVE (Common Vulnerabilities and Exposures) rilevati su Amazon Linux Security Center. Le patch CVE vengono applicate automaticamente entro 30 giorni dal rilascio, come mostrato in Amazon Linux Security Center. Le patch vengono installate durante il programma di manutenzione del gateway, a condizione che il gateway sia online.
Storage Gateway non supporta l'aggiornamento manuale di un EC2 gateway Amazon utilizzando le direttive cloud-init. Se utilizzi questo metodo per aggiornare un gateway, potresti riscontrare problemi di interoperabilità che ti impediscono di attivare o utilizzare l'appliance gateway.

Frequenza di aggiornamento e comportamento previsto

AWS aggiorna il componente dei servizi cloud in base alle esigenze senza causare interruzioni ai gateway implementati. I dispositivi gateway distribuiti ricevono i seguenti tipi di aggiornamenti:

- Manutenzione: aggiornamenti regolari che possono includere aggiornamenti del sistema operativo e del software, correzioni relative a stabilità, prestazioni e sicurezza e accesso a nuove funzionalità.
- Urgente: aggiornamenti critici che includono le correzioni necessarie per problemi che hanno un impatto immediato sulla sicurezza, le prestazioni o la durabilità del gateway. Gli aggiornamenti urgenti possono essere rilasciati in qualsiasi momento, al di fuori della normale cadenza degli aggiornamenti mensili di manutenzione e funzionalità.

Tutti gli aggiornamenti sono cumulativi e, se applicati, aggiornano i gateway alla versione corrente. Per informazioni sulle modifiche specifiche incluse in ogni aggiornamento, consulta le note di rilascio per il software Gateway Appliance.

Tutti gli aggiornamenti delle appliance gateway possono causare una breve interruzione del servizio. Non è necessario riavviare l'host VM del gateway durante gli aggiornamenti, ma il gateway non sarà disponibile per un breve periodo durante l'aggiornamento e il riavvio dell'appliance gateway.

Quando si installa e si attiva il gateway, viene impostata una finestra di manutenzione predefinita. È possibile modificare la pianificazione della finestra di manutenzione in qualsiasi momento. Puoi anche disattivare gli aggiornamenti di manutenzione, ma ti consigliamo di lasciarli attivi.

> **Note**
>
> Gli aggiornamenti urgenti verranno applicati in base alla pianificazione della finestra di manutenzione, anche se gli aggiornamenti di manutenzione regolari sono disattivati.

Prima di applicare qualsiasi aggiornamento al gateway, ti AWS avvisa con un messaggio sulla console di Storage Gateway e sul tuo AWS Health Dashboard. Per ulteriori informazioni, consulta AWS Health Dashboard. Per modificare l'indirizzo e-mail a cui vengono inviate le notifiche di aggiornamento del software, consulta Aggiornare i contatti alternativi per l' AWS account nella Guida di riferimento per la gestione degli AWS account.

Quando gli aggiornamenti sono disponibili, nella scheda Dettagli del gateway viene visualizzato un messaggio di manutenzione. È inoltre possibile visualizzare la data e l'ora in cui è stato applicato l'ultimo aggiornamento riuscito nella scheda Dettagli.

Attiva o disattiva gli aggiornamenti di manutenzione

Quando gli aggiornamenti di manutenzione sono attivati, il gateway li applica automaticamente in base alla pianificazione della finestra di manutenzione configurata. Per ulteriori informazioni, vedere Modificare la pianificazione della finestra di manutenzione del gateway Modificare la pianificazione .

Se gli aggiornamenti di manutenzione sono disattivati, il gateway non li applicherà automaticamente, ma è sempre possibile applicarli manualmente utilizzando la console, l'API o la CLI di Storage Gateway. A volte vengono applicati aggiornamenti urgenti durante la finestra di manutenzione configurata, indipendentemente da questa impostazione.

> **Note**
>
> La procedura seguente descrive come attivare o disattivare gli aggiornamenti del gateway utilizzando la console Storage Gateway. Per modificare questa impostazione a livello di codice utilizzando l'API, vedere UpdateMaintenanceStartTimelo Storage Gateway API Reference.

Per attivare o disattivare gli aggiornamenti di manutenzione utilizzando la console Storage Gateway:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi scegli il gateway per il quale desideri configurare gli aggiornamenti di manutenzione.
3. Scegli Azioni, quindi scegli Modifica impostazioni di manutenzione.
4. Per gli aggiornamenti di manutenzione, seleziona Attivato o Disattivato.
5. Al termine, scegli Salva modifiche.

È possibile verificare l'impostazione aggiornata nella scheda Dettagli per il gateway selezionato nella console Storage Gateway.

Modifica la pianificazione della finestra di manutenzione del gateway

Se gli aggiornamenti di manutenzione sono attivati, il gateway li applica automaticamente in base alla pianificazione della finestra di manutenzione. A volte vengono applicati aggiornamenti urgenti durante la finestra di manutenzione configurata, indipendentemente dall'impostazione degli aggiornamenti di manutenzione.

> **Note**
>
> La procedura seguente descrive come modificare la pianificazione della finestra di manutenzione utilizzando la console Storage Gateway. Per modificare questa impostazione a livello di codice utilizzando l'API, vedere UpdateMaintenanceStartTimelo Storage Gateway API Reference.

Per modificare la pianificazione della finestra di manutenzione utilizzando la console Storage Gateway:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi scegli il gateway per il quale desideri configurare gli aggiornamenti di manutenzione.
3. Scegli Azioni, quindi scegli Modifica impostazioni di manutenzione.
4. In Ora di inizio della finestra di manutenzione, procedi come segue:

a. Per Pianificazione, scegli Settimanale o Mensile per impostare la cadenza della finestra di manutenzione.

b. Se scegli Settimanale, modifica i valori di Giorno della settimana e Ora per impostare il momento specifico durante ogni settimana in cui inizierà la finestra di manutenzione.

   Se scegli Mensile, modifica i valori di Giorno del mese e Ora per impostare il momento specifico durante ogni mese in cui inizierà la finestra di manutenzione.

   > **Note**
   >
   > Il valore massimo che può essere impostato per il giorno del mese è 28. Non è possibile impostare il programma di manutenzione in modo che inizi nei giorni dal 29 al 31.
   > Se si verifica un errore durante la configurazione di questa impostazione, è possibile che il software del gateway non sia aggiornato. Valuta la possibilità di aggiornare prima il gateway manualmente e poi di riprovare a configurare la pianificazione della finestra di manutenzione.

5. Al termine, scegli Salva le modifiche.

È possibile verificare le impostazioni aggiornate nella scheda Dettagli per il gateway selezionato nella console Storage Gateway.

Applica un aggiornamento manualmente

Se è disponibile un aggiornamento software per il gateway, è possibile applicarlo manualmente seguendo la procedura riportata di seguito. Questo processo di aggiornamento manuale ignora la pianificazione della finestra di manutenzione e applica l'aggiornamento immediatamente, anche se gli aggiornamenti di manutenzione sono disattivati.

> **Note**
>
> La procedura seguente descrive come applicare manualmente un aggiornamento utilizzando la console Storage Gateway. Per eseguire questa azione a livello di codice utilizzando l'API, vedere UpdateGatewaySoftwareNowlo Storage Gateway API Reference.

Per applicare manualmente un aggiornamento software del gateway utilizzando la console Storage Gateway:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi scegli il gateway che desideri aggiornare.

   Se è disponibile un aggiornamento, la console visualizza un banner di notifica blu nella scheda Dettagli del gateway, che include un'opzione per applicare l'aggiornamento.
3. Scegli Applica aggiornamento ora per aggiornare immediatamente il gateway.

> **Note**
>
> Questa operazione causa un'interruzione temporanea della funzionalità del gateway durante l'installazione dell'aggiornamento. Durante questo periodo, lo stato del gateway appare OFFLINE nella console Storage Gateway. Al termine dell'installazione dell'aggiornamento, il gateway riprende il normale funzionamento e il suo stato passa a RUNNING.

È possibile verificare che il software del gateway sia stato aggiornato alla versione più recente controllando la scheda Dettagli per il gateway selezionato nella console Storage Gateway.

Esecuzione delle attività di manutenzione utilizzando la console locale

Questa sezione contiene i seguenti argomenti, che forniscono informazioni su come eseguire le attività di manutenzione utilizzando la console locale dell'appliance gateway. Puoi eseguire queste attività accedendo alla console locale tramite la macchina virtuale locale o l' EC2 istanza Amazon che ospita il tuo dispositivo gateway. La maggior parte delle attività è comune tra le diverse piattaforme host, ma ci sono anche alcune differenze.

Argomenti

- Accesso alla console locale del gateway- Scopri come accedere alla console locale per un gateway locale ospitato su una macchina virtuale (KVM) basata su Linux Kernel VMware ESXi o una piattaforma Microsoft Hyper-V Manager.

- Esecuzione di attività sulla console locale della macchina virtuale- Scopri come utilizzare la console locale per eseguire attività di configurazione di base e avanzate per un gateway locale, come la configurazione di un proxy HTTP, la visualizzazione dello stato delle risorse di sistema o l'esecuzione di comandi da terminale.
- Esecuzione di attività sulla console locale del EC2 gateway Amazon- Scopri come accedere alla console locale per eseguire attività di configurazione di base e avanzate per un EC2 gateway Amazon, come configurare un proxy HTTP, visualizzare lo stato delle risorse di sistema o eseguire comandi da terminale.

Accesso alla console locale del gateway

L'accesso alla console locale di una VM dipende dal tipo di Hypervisor su cui è stata distribuita la VM del gateway. In questa sezione, puoi trovare informazioni su come accedere alla console locale della macchina virtuale utilizzando Linux Kernel-based Virtual Machine (KVM) VMware ESXi e Microsoft Hyper-V Manager.

Argomenti

- Accesso alla console locale del gateway con Linux KVM
- Accesso alla console locale del gateway con VMware ESXi
- Accesso alla console locale del gateway con Microsoft Hyper-V

Accesso alla console locale del gateway con Linux KVM

Esistono diversi modi per configurare le macchine virtuali in esecuzione su KVM, a seconda della distribuzione Linux utilizzata. Istruzioni per accedere alle opzioni di configurazione KVM dalla riga di comando. Le istruzioni potrebbero differire a seconda dell'implementazione KVM.

Per accedere alla console locale del gateway con KVM

1. Usa il seguente comando per elencare VMs quelli attualmente disponibili in KVM.

   ```
   # virsh list
   ```

   Il comando restituisce un elenco di informazioni relative VMs all'ID, al nome e allo stato per ciascuna di esse. Annota `Id` la macchina virtuale per la quale desideri avviare la console locale del gateway.

2. Utilizzare il comando seguente per accedere alla console locale.

```
# virsh console Id
```

Sostituisci *Id* con l'ID della macchina virtuale annotato nel passaggio precedente.

La console locale di AWS Appliance gateway richiede di effettuare il login per modificare la configurazione di rete e altre impostazioni.

3. Immettete il nome utente e la password per accedere alla console locale del gateway. Per ulteriori informazioni, vedere Accesso alla console locale File Gateway Accesso alla console locale .

Dopo aver effettuato l'accesso, viene visualizzato il menu Attivazione AWS dell'appliance - Configurazione. È possibile selezionare le opzioni del menu per eseguire le attività di configurazione del gateway. Per ulteriori informazioni, vedere Esecuzione di attività sulla console locale della macchina virtuale .

Accesso alla console locale del gateway con VMware ESXi

Per accedere alla console locale del gateway con VMware ESXi

1. Nel client VMware vSphere, selezionare la macchina virtuale gateway.
2. Assicurati che la VM gateway sia accesa.

> **Note**
>
> Se la macchina virtuale gateway è accesa, viene visualizzata un'icona a forma di freccia verde con l'icona della macchina virtuale nel pannello del browser della macchina virtuale sul lato sinistro della finestra dell'applicazione. Se la tua VM gateway non è accesa, puoi accenderla scegliendo l'icona verde Power On sulla barra degli strumenti nella parte superiore della finestra dell'applicazione.

3. Scegli la scheda Console nel pannello delle informazioni principale sul lato destro della finestra dell'applicazione.

Dopo alcuni istanti, la console locale del gateway dell' AWS appliance richiede di accedere per modificare la configurazione di rete e altre impostazioni.

> **Note**
>
> Per rilasciare il cursore dalla finestra della console, premi Ctrl+Alt.

4. Immettete il nome utente e la password per accedere alla console locale del gateway. Per ulteriori informazioni, vedere Accesso alla console locale File Gateway Accesso alla console locale .

   Dopo aver effettuato l'accesso, viene visualizzato il menu Attivazione AWS dell'appliance - Configurazione. È possibile selezionare le opzioni del menu per eseguire le attività di configurazione del gateway. Per ulteriori informazioni, vedere Esecuzione di attività sulla console locale della macchina virtuale .

Accesso alla console locale del gateway con Microsoft Hyper-V

Per accedere alla console locale del gateway (Microsoft Hyper-V)

1. Seleziona la macchina virtuale dell'appliance gateway dal pannello Macchine virtuali sul lato sinistro della finestra dell'applicazione Microsoft Hyper-V Manager.
2. Verifica che il gateway sia attivo.

> **Note**
>
> Se la macchina virtuale gateway è accesa, `Running` viene visualizzata nella colonna Stato della macchina virtuale nel pannello Macchine virtuali sul lato sinistro della finestra dell'applicazione. Se la VM gateway non è accesa, puoi attivarla scegliendo Avvia nel pannello Azioni sul lato destro della finestra dell'applicazione.

3. Scegliete Connect dal pannello Azioni.

   Verrà visualizzata la finestra Virtual Machine Connection (Connessione macchina virtuale). Se viene visualizzata una finestra di autenticazione, digitare le credenziali di accesso fornite dall'amministratore dell'hypervisor.

   Dopo alcuni istanti, la console locale del gateway dell' AWS appliance richiede di effettuare il login per modificare la configurazione di rete e altre impostazioni.

4. Immettete il nome utente e la password per accedere alla console locale del gateway. Per ulteriori informazioni, vedere Accesso alla console locale File Gateway Accesso alla console locale .

   Dopo aver effettuato l'accesso, viene visualizzato il menu Attivazione AWS dell'appliance - Configurazione. È possibile selezionare le opzioni del menu per eseguire le attività di configurazione del gateway. Per ulteriori informazioni, vedere Esecuzione di attività sulla console locale della macchina virtuale .

Esecuzione di attività sulla console locale della macchina virtuale

Per un File Gateway distribuito in locale, è possibile eseguire le seguenti attività di manutenzione utilizzando la console locale dell'host VM. Queste attività sono comuni agli VMware hypervisor Microsoft Hyper-V e Linux Kernel-based Virtual Machine (KVM).

Argomenti

- Accesso alla console locale File Gateway- Scopri come accedere alla console locale dove puoi configurare le impostazioni di rete del gateway e modificare la password predefinita.
- Configurazione di un proxy HTTP- Scopri come configurare Storage Gateway per instradare tutto il traffico AWS degli endpoint attraverso un server proxy.
- Configurazione delle impostazioni di rete del gateway- Scopri come configurare il gateway per utilizzare DHCP o un indirizzo IP statico.
- Verifica della connettività di rete del gateway- Scopri come utilizzare la console locale del gateway per testare la connettività di rete.
- Visualizzazione dello stato relativo alle risorse di sistema del gateway- Scopri come controllare i core della CPU virtuale, le dimensioni del volume root e la RAM del gateway.
- Configurazione di un server Network Time Protocol (NTP) per il gateway- Scopri come visualizzare e modificare le configurazioni del server NTP (Network Time Protocol) e sincronizzare l'ora del gateway con l'host dell'hypervisor.
- Esecuzione di comandi Storage Gateway sulla console locale- Scopri come eseguire i comandi della console locale per eseguire attività come il salvataggio delle tabelle di routing, la connessione e altro ancora. Supporto

Accesso alla console locale File Gateway

Quando la VM è pronta per l'accesso, è visualizzata la schermata di autenticazione. Se è la prima volta che accedi alla console locale della macchina virtuale, usi le credenziali di accesso temporanee per accedere. Queste credenziali temporanee consentono di accedere ai menu in cui è possibile configurare le impostazioni di rete del gateway e modificare la password dalla console locale. Il nome utente iniziale è `admin` e la password temporanea è. `password` È necessario modificare la password al primo accesso.

Per modificare la password temporanea

1. Nel menu principale AWS Appliance Activation - Configuration, immettere il numero corrispondente per Gateway Console.
2. Esegui il comando `passwd`. Per informazioni su come eseguire il comando, consulta Esecuzione di comandi Storage Gateway sulla console locale.

Impostazione della password della console locale dalla console Storage Gateway

È inoltre possibile gestire la password della console locale dalla console basata sul Web di Storage Gateway. Qualsiasi aggiornamento della password eseguito con successo con la console basata sul Web sostituirà la password utilizzata dalla console locale della VM del gateway, inclusa la password temporanea se non è mai stato effettuato l'accesso localmente. Se il gateway non è attualmente raggiungibile tramite la rete, il processo di aggiornamento della password avrà esito negativo.

Per impostare la password della console locale sulla console Storage Gateway

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi seleziona il gateway per il quale desideri impostare una nuova password.
3. In Actions (Operazioni), selezionare Set Local Console Password (Imposta la password della console locale).
4. Nella finestra di dialogo di Set Local Console Password (Imposta la password della console locale), digitare la nuova password, poi confermarla e, infine, selezionare Save (Salva).

   La nuova password sostituisce la password attuale. Il servizio Storage Gateway non salva, archivia o registra la password, ma la trasmette in modo sicuro tramite un canale crittografato alla macchina virtuale, dove viene archiviata in modo sicuro.

> **Note**
>
> La password può essere composta da qualsiasi carattere sulla tastiera e può contenere da 1 a 512 caratteri.

Configurazione di un proxy HTTP

I File Gateway supportano la configurazione di un proxy HTTP.

> **Note**
>
> L'unica configurazione proxy supportata da File Gateway è HTTP.

Se il gateway deve usare un server proxy per comunicare con Internet, devi configurare le impostazioni del proxy HTTP per il gateway. A tale scopo, basta specificare un indirizzo IP e un numero di porta per l'host che esegue il proxy. Dopo averlo fatto, Storage Gateway indirizza tutto il traffico AWS degli endpoint attraverso il server proxy. Le comunicazioni tra il gateway e gli endpoint sono crittografate, anche quando si utilizza il proxy HTTP. Per informazioni sui requisiti di rete del gateway, consulta Requisiti di rete e firewall.

Per configurare un proxy HTTP per un File Gateway

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale per la macchina virtuale basata su kernel Linux (KVM), consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, immettere il numero corrispondente per selezionare Configurazione del proxy HTTP.
3. Dal menu di Configurazione del proxy HTTP per l'attivazione dell'appliance AWS , immettere il numero corrispondente per l'operazione che si desidera eseguire:

- Configurazione del proxy HTTP: specificare un nome host e una porta per completare la configurazione.
- Visualizzazione della configurazione del proxy HTTP corrente: se il proxy HTTP non è configurato, viene visualizzato il messaggio `HTTP Proxy not configured`. Se un proxy HTTP è configurato, vengono visualizzati il nome host e la porta del proxy HTTP.
- Rimozione di una configurazione del proxy HTTP: viene visualizzato il messaggio `HTTP Proxy Configuration Removed`.

4. Per applicare le impostazioni della configurazione HTTP, riavviare la VM.

Configurazione delle impostazioni di rete del gateway

L'impostazione predefinita per la configurazione di rete del gateway è DHCP (Dynamic Host Configuration Protocol). Con DHCP, al gateway viene assegnato automaticamente un indirizzo IP. In alcuni casi, può essere necessario assegnare manualmente un indirizzo IP statico al gateway, come descritto di seguito.

Per configurare il gateway affinché utilizzi indirizzi IP statici

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale Attivazione dell'AWS appliance - Configurazione, immettere il numero corrispondente per selezionare Configurazione di rete.
3. Dal menu Network Configuration, effettuate una delle seguenti operazioni:

Per eseguire questa operazione	eseguire questa operazione
Ottenere informazioni sulla scheda di rete	Immettere il numero corrispondente per selezionare Descrivi adattatore.

Per eseguire questa operazione	eseguire questa operazione
	Viene visualizzato un elenco di nomi di adattatore e viene richiesto di immettere un nome di adattatore, ad esempio. **`eth0`** Se la scheda specificata è in uso, vengono mostrate le seguenti informazioni: • Indirizzo MAC (Media Access Control) • IP address (Indirizzo IP) • Netmask • Indirizzo IP del gateway • Stato DHCP abilitato I nomi degli adattatori elencati qui vengono utilizzati quando si configura un indirizzo IP statico o quando si imposta l'adattatore predefinito del gateway.
Configura il routing DHCP	Inserisci il numero corrispondente per seleziona re Configura DHCP. Per l'utilizzo di DHCP, viene richiesto di configurare l'interfaccia di rete.

Per eseguire questa operazione	eseguire questa operazione
Configurare un indirizzo IP statico per il gateway	Inserisci il numero corrispondente per seleziona re Configura IP statico. Per configurare un indirizzo IP statico, viene chiesto di digitare le informazioni riportate di seguito: • Nome scheda di rete • IP address (Indirizzo IP) • Netmask • Indirizzo del gateway predefinito • Indirizzo DNS (Domain Name Service) primario • Indirizzo DNS (Domain Name Service) secondario **Important** Se il gateway è già stato attivato, affinché le impostazioni abbiano effetto è necessario arrestarlo e riavviarlo dalla console Storage Gateway. Per ulteriori informazioni, consulta Spegnimento della macchina virtuale gateway.

Per eseguire questa operazione	eseguire questa operazione
	Se il gateway utilizza più di un'interfaccia di rete, è necessario impostare tutte le interfacce attive per utilizzare DHCP o indirizzi IP statici. Ad esempio, supponiamo che la VM del gateway utilizzi due interfacce configurate come DHCP. Se in un secondo momento si imposta un'interfaccia con un IP statico, l'altra interfaccia viene disattivata. Per riattivarla, sarà necessario configurarla con un indirizzo IP statico. Se entrambe le interfacce sono inizialmente configurate per l'utilizzo di indirizzi IP statici e poi si imposta il gateway in modo che si avvalga di DHCP, entrambe le interfacce, infine, utilizzeranno DHCP.

Per eseguire questa operazione	eseguire questa operazione
Configura un nome host per il gateway	Immettere il numero corrispondente per selezionare Configura nome host. Ti viene richiesto di scegliere se il gateway utilizzerà un nome host statico specificato dall'utente o ne acquisirà uno automaticamente tramite DCHP o rDNS. Se si seleziona Statico, viene richiesto di fornire un nome host statico, ad esempio. `testgateway.example.com` Inserisci y per applicare la configurazione. **Note** Se configuri un nome host statico per il gateway, assicurati che il nome host fornito si trovi nel dominio a cui è unito il gateway. È inoltre necessario creare un record A nel sistema DNS che punti l'indirizzo IP del gateway al relativo nome host statico.
Visualizza la configurazione del nome host del gateway	Inserisci il numero corrispondente per seleziona re Visualizza la configurazione del nome host. Vengono visualizzati il nome host, la modalità di acquisizione, il dominio e il realm di Active Directory del gateway.

Per eseguire questa operazione	eseguire questa operazione
Reimpostare tutte le configurazioni di rete del gateway su DHCP	Immettere il numero corrispondente per selezionare Reimposta tutto su DHCP. Tutte le interfacce di rete sono impostate per l'utilizzo di DHCP. **Important** Se il gateway è già stato attivato, affinché le impostazioni abbiano effetto è necessario arrestare il gateway stesso e riavviarlo dalla console Storage Gateway. Per ulteriori informazioni, consulta Spegnimento della macchina virtuale gateway.
Impostare l'adattatore di routing predefinito del gateway	Immettere il numero corrispondente per selezionare Imposta scheda predefinita. Vengono visualizzati gli adattatori disponibili per il gateway e viene richiesto di scegliere uno degli adattatori, ad esempio. **`eth0`**
Modificare la configurazione DNS del gateway	Inserisci il numero corrispondente per seleziona re Modifica configurazione DNS. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. Viene richiesto di fornire il nuovo indirizzo IP.

Per eseguire questa operazione	eseguire questa operazione
Visualizzare la configurazione DNS del gateway	Immettere il numero corrispondente per selezionare Visualizza configurazione DNS. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. **Note** Per alcune versioni dell' VMware hypervisor, puoi modificare la configura zione dell'adattatore in questo menu.
Visualizzare le tabelle di routing	Immettere il numero corrispondente per selezionare Visualizza instradamenti. Viene visualizzato l'instradamento predefinito del gateway.

Verifica della connettività di rete del gateway

Puoi utilizzare la console locale del gateway per testare la connettività di rete. Questo test può essere utile per risolvere eventuali problemi di rete del gateway.

Per testare la connettività di rete del gateway

1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.

2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Verifica connettività di rete.

   Se il gateway è già stato attivato, il test di connettività inizia immediatamente. Per i gateway che non sono ancora stati attivati, è necessario specificare il tipo di endpoint e procedere Regione AWS come descritto nei passaggi seguenti.
3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se hai selezionato il tipo di endpoint pubblico, inserisci il numero corrispondente per selezionare Regione AWS quello che desideri testare. Per gli endpoint supportati Regioni AWS e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere Gateway di archiviazione AWS endpoint e quote nel. Riferimenti generali di AWS

Man mano che il test procede, ogni endpoint visualizza [PASSED] o [FAILED], indicando lo stato della connessione nel modo seguente:

Messaggio	Description
[PASSED]	Storage Gateway dispone di connettività di rete.
[FAILED]	Storage Gateway non dispone di connettività di rete.

Visualizzazione dello stato relativo alle risorse di sistema del gateway

Quando viene avviato, il gateway verifica i core CPU virtuali, la dimensione del volume root e la RAM. Quindi stabilisce se tali risorse di sistema sono sufficienti per il corretto funzionamento del gateway. I risultati di questi controlli sono riportati nella console locale del gateway.

Per visualizzare lo stato di un controllo delle risorse di sistema

1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla VMware ESXi console, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.

- Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.

2. Dal menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero corrispondente per selezionare Visualizzazione del controllo relativo alle risorse di sistema.

   Ogni risorsa visualizza [OK], [ATTENZIONE] o [ERRORE], che indicano lo stato della risorsa nel modo seguente:

Messaggio	Description
[OK]	La risorsa ha superato il controllo delle risorse di sistema.
[WARNING]	La risorsa non soddisfa i requisiti raccomandati, ma il gateway può continuare a funzionare. Storage Gateway mostra un messaggio che descrive i risultati del controllo delle risorse.
[FAIL]	La risorsa non soddisfa i requisiti minimi. Il gateway potrebbe non funzionare correttamente. Storage Gateway mostra un messaggio che descrive i risultati del controllo delle risorse.

   La console visualizza inoltre il numero di errori e avvisi accanto all'opzione del menu di controllo delle risorse.

Configurazione di un server Network Time Protocol (NTP) per il gateway

Puoi visualizzare e modificare le configurazioni del server Network Time Protocol (NTP) e sincronizzare l'ora della VM associata al gateway con l'host dell'hypervisor.

Per gestire l'ora di sistema

1. Accedere alla console locale del gateway:

- Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedereAccesso alla console locale del gateway con VMware ESXi.
- Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
- Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.

2. Dal menu principale Attivazione dell'AWS appliance - Configurazione, immettere il numero corrispondente per selezionare System Time Management.
3. Dal menu System Time Management, immettete il numero corrispondente per eseguire una delle seguenti attività.

Per eseguire questa operazione	eseguire questa operazione
Visualizza e sincronizza l'ora della VM con quella del server NTP.	Immettete il numero corrispondente per selezionare Visualizza e sincronizza l'ora di sistema. Viene visualizzata l'ora corrente della VM. Il File Gateway determina la differenza di fuso orario rispetto alla VM del gateway e l'ora del server NTP richiede di sincronizzare l'ora della VM con l'ora NTP. Dopo la distribuzione e l'esecuzione del gateway, in alcune situazioni l'ora impostata sulla VM a esso associata può presentare degli scostamenti. Ad esempio, se si verifica un'interruzione di rete prolungata e l'host dell'hypervisor e il gateway non ricevono gli aggiornamenti dell'ora, l'ora della VM del gateway divergerà dall'ora esatta. Quando si verifica uno scostamento dell'ora, si genera una discrepanza tra l'ora di esecuzione indicata in caso di operazioni quali gli snapshot e l'ora

Per eseguire questa operazione	eseguire questa operazione
	effettiva alla quale le operazioni vengono eseguite. Per un gateway distribuito su VMware ESXi, è sufficiente impostare l'ora dell'host dell'hype rvisor e sincronizzare l'ora della VM con l'host per evitare variazioni di orario. Per ulteriori informazioni, consulta Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware . In caso, invece, di gateway distribuito su Microsoft Hyper-V, è necessario controllare periodicamente l'ora impostata sulla VM. Per ulteriori informazioni, consulta Sincronizza l'ora della macchina virtuale con l'ora dell'host KVM Hyper-V o Linux. Per un gateway distribuito su KVM, è possibile controllare e sincronizzare l'ora della macchina virtuale utilizzando l'interfaccia della riga di comando `virsh` per KVM.
Modifica della configurazione del server NTP	Immettere il numero corrispondente per selezionare Modifica configurazione NTP. Ti viene richiesto di fornire un server NTP preferito e un server secondario.
Visualizzazione della configurazione del server NTP	Immettere il numero corrispondente per selezionare Visualizza configurazione NTP. Viene visualizzata la configurazione del server NTP.

Esecuzione di comandi Storage Gateway sulla console locale

La console locale della VM in Storage Gateway offre un ambiente sicuro per la configurazione e la diagnostica dei problemi del gateway. Utilizzando i comandi della console locale, è possibile eseguire attività di manutenzione come il salvataggio delle tabelle di routing, la connessione e così via. Supporto

Per eseguire un comando di diagnostica o di configurazione

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedere. Accesso alla console locale del gateway con VMware ESXi
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero corrispondente per selezionare Console del gateway.
3. Dal prompt dei comandi della console del gateway, immettere **h**.

   La console mostra il menu COMANDI DISPONIBILI che elenca i comandi disponibili:

Comando	Funzione
dig	Raccogli l'output da dig per la risoluzione dei problemi DNS.
Esci	Torna al menu di configurazione.
h	Visualizza l'elenco dei comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console

Comando	Funzione
	Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere della rete gateway.
ip	Mostra/manipola routing, dispositivi e tunnel. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere .
iptables	Strumento di amministrazione per il filtraggio dei IPv4 pacchetti e NAT.
tabelle ip6	Strumento di amministrazione per il filtraggio dei IPv6 pacchetti e NAT.
ncport	Verifica la connettività a una porta TCP specifica su una rete.
nping	Raccogli l'output da nping per la risoluzione dei problemi di rete.
open-support-channel	Connect to AWS Support. Per istruzioni su come attivare l'accesso al AWS supporto, vedi Vuoi che il AWS supporto ti aiuti a risolvere i problemi del EC2 gateway Vuoi che il AWS del gateway. EC2
passwd	Aggiorna i token di autenticazione.
save-iptables	Tabelle IP persistenti.

Comando	Funzione
save-routing-table	Salva la voce della tabella di routing appena aggiunta.
tcptraceroute	Raccogli l'output del traceroute sul traffico TCP verso una destinazione.
sslcheck	Restituisce l'output con l'emittente del certifica to **Note** Storage Gateway utilizza la verifica dell'emittente del certificato e non supporta l'ispezione SSL. Se questo comando restituisce un emittente diverso da aws-appliance@amaz on.com, è probabile che sia un'applic azione che esegue un'ispezione ssl. In tal caso, si consiglia di ignorare l'ispezione SSL per l'appliance Storage Gateway.

4. Dal prompt dei comandi della console del gateway, immettere il comando corrispondente alla funzione che si desidera utilizzare e seguire le istruzioni.

Per informazioni su un comando, digitare **`man`** + *`command name`* al prompt dei comandi.

Esecuzione di attività sulla console locale del EC2 gateway Amazon

Alcune attività di manutenzione richiedono l'accesso alla console locale quando si esegue un gateway distribuito su un' EC2 istanza Amazon. Questa sezione descrive come accedere alla console locale ed eseguire attività di manutenzione.

Argomenti

- Accesso alla console locale Amazon EC2 Gateway- Scopri come connetterti e accedere alla console locale del gateway, la tua EC2 istanza Amazon, utilizzando un client Secure Shell (SSH).
- Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP- Scopri come configurare un proxy Socket Secure versione 5 (SOCKS5) tra AWS e un gateway distribuito su un' EC2 istanza Amazon.
- Verifica della connettività di rete del gateway- Scopri come utilizzare la console locale del gateway per testare la connettività di rete tra il gateway e varie risorse di rete.
- Visualizzazione dello stato relativo alle risorse di sistema del gateway- Scopri come utilizzare la console locale del gateway per controllare i core della CPU virtuale, le dimensioni del volume root e la RAM del gateway.
- Esecuzione dei comandi Storage Gateway sulla console locale per un EC2 gateway Amazon- Scopri come eseguire i comandi della console locale per eseguire attività come il salvataggio delle tabelle di routing, la connessione e altro Supporto ancora.
- Configurazione delle impostazioni di rete Amazon EC2 gateway- Scopri come utilizzare la console locale per visualizzare e configurare impostazioni di rete come DNS e nome host per un gateway su un'istanza Amazon EC2 .

Accesso alla console locale Amazon EC2 Gateway

Accedi alla console locale del gateway su un' EC2 istanza Amazon utilizzando un client Secure Shell (SSH). Per informazioni dettagliate, consulta Connect to your istance nella Amazon EC2 User Guide. Per connetterti in questo modo, avrai bisogno della coppia di chiavi SSH specificata all'avvio dell'istanza. Per informazioni sulle coppie di EC2 chiavi Amazon, consulta le coppie di EC2 chiavi Amazon nella Amazon EC2 User Guide.

Accedere alla console locale del gateway

1. Connect all' EC2 istanza Amazon tramite SSH e accedi come utente amministratore.
2. Dopo aver effettuato l'accesso, viene visualizzato il menu principale AWS Appliance Activation - Configuration, da cui è possibile eseguire varie attività.

Per ulteriori informazioni su questa attività	vedere questo argomento
Configurare un proxy HTTP per il gateway	Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP

Per ulteriori informazioni su questa attività	vedere questo argomento
Configurazione delle impostazioni di rete per il gateway	Configurazione delle impostazioni di rete Amazon EC2 gateway
Verificare la connettività di rete	Verifica della connettività di rete del gateway
Visualizzare un controllo delle risorse di sistema	Visualizzazione dello stato relativo alle risorse di sistema del gateway.
Esecuzione dei comandi della console Storage Gateway	Esecuzione dei comandi Storage Gateway sulla console locale per un EC2 gateway Amazon

Per arrestare il gateway, digitare **0**.

Per uscire dalla sessione di configurazione, digitare **X**.

Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP

Storage Gateway supporta la configurazione di un proxy Socket Secure versione 5 (SOCKS5) tra il gateway distribuito su Amazon EC2 e AWS.

Se il gateway deve usare un server proxy per comunicare con Internet, devi configurare le impostazioni del proxy HTTP per il gateway. A tale scopo, basta specificare un indirizzo IP e un numero di porta per l'host che esegue il proxy. Dopo averlo fatto, Storage Gateway indirizza tutto il traffico AWS degli endpoint attraverso il server proxy. Le comunicazioni tra il gateway e gli endpoint sono crittografate, anche quando si utilizza il proxy HTTP.

Per instradare il traffico Internet del gateway attraverso un server proxy locale

1. Accedere alla console locale del gateway. Per istruzioni, consulta Accesso alla console locale Amazon EC2 Gateway.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, immettere il numero corrispondente per selezionare Configurazione del proxy HTTP.
3. Dal menu di Configurazione del proxy HTTP per l'attivazione dell'appliance AWS , immettere il numero corrispondente per l'operazione che si desidera eseguire:

- Configurazione del proxy HTTP: specificare un nome host e una porta per completare la configurazione.
- Visualizzazione della configurazione del proxy HTTP corrente: se il proxy HTTP non è configurato, viene visualizzato il messaggio `HTTP Proxy not configured`. Se un proxy HTTP è configurato, vengono visualizzati il nome host e la porta del proxy HTTP.
- Rimozione di una configurazione del proxy HTTP: viene visualizzato il messaggio `HTTP Proxy Configuration Removed`.

Verifica della connettività di rete del gateway

Puoi utilizzare la console locale del gateway per testare la connettività di rete. Questo test può essere utile per risolvere eventuali problemi di rete del gateway.

Per testare la connettività del gateway

1. Accedere alla console locale del gateway. Per istruzioni, consulta Accesso alla console locale Amazon EC2 Gateway.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Verifica connettività di rete.

   Se il gateway è già stato attivato, il test di connettività inizia immediatamente. Per i gateway che non sono ancora stati attivati, è necessario specificare il tipo di endpoint e procedere Regione AWS come descritto nei passaggi seguenti.
3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se hai selezionato il tipo di endpoint pubblico, inserisci il numero corrispondente per selezionare Regione AWS quello che desideri testare. Per gli endpoint supportati Regioni AWS e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere Gateway di archiviazione AWS endpoint e quote nel. Riferimenti generali di AWS

Man mano che il test procede, ogni endpoint visualizza [PASSED] o [FAILED], indicando lo stato della connessione nel modo seguente:

Messaggio	Description
[PASSED]	Storage Gateway dispone di connettività di rete.
[FAILED]	Storage Gateway non dispone di connettività di rete.

Visualizzazione dello stato relativo alle risorse di sistema del gateway

All'avvio, File Gateway controlla i core della CPU virtuale, le dimensioni del volume root e la RAM. Quindi determina se le risorse di sistema disponibili sono sufficienti per il corretto funzionamento del gateway. È possibile visualizzare i risultati del controllo delle risorse di sistema utilizzando la console locale del gateway.

Per visualizzare lo stato di un controllo delle risorse di sistema

1. Accedi alla console locale sul tuo Amazon EC2 File Gateway. Per istruzioni, consulta Accesso alla console locale Amazon EC2 Gateway.
2. Nel menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero seriale corrispondente per selezionare Visualizzazione del controllo relativo alle risorse di sistema.

   La console locale del gateway visualizza [OK], [WARNING] o [FAIL] per indicare lo stato della risorsa nel modo seguente:

Messaggio	Description
[OK]	La risorsa ha superato il controllo delle risorse di sistema.
[WARNING]	La risorsa non soddisfa i requisiti consigliati, ma il gateway può continuare a funzionare. La console locale del gateway visualizza un messaggio che descrive i risultati del controllo delle risorse.
[FAIL]	La risorsa non soddisfa i requisiti minimi. Il gateway potrebbe non funzionare correttam

Messaggio	Description
	ente. La console locale del gateway visualizza un messaggio che descrive i risultati del controllo delle risorse.

La console locale visualizza anche il numero di errori e avvisi accanto all'opzione del menu di controllo delle risorse.

Esecuzione dei comandi Storage Gateway sulla console locale per un EC2 gateway Amazon

La Gateway di archiviazione AWS console aiuta a fornire un ambiente sicuro per la configurazione e la diagnosi dei problemi relativi al gateway. Utilizzando i comandi della console, è possibile eseguire attività di manutenzione come il salvataggio delle tabelle di routing o la connessione a. Supporto

Per eseguire un comando di diagnostica o di configurazione

1. Accedere alla console locale del gateway. Per istruzioni, consulta Accesso alla console locale Amazon EC2 Gateway.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Console del Gateway.
3. Dal prompt dei comandi della console del gateway, immettere **h**.

   La console mostra il menu COMANDI DISPONIBILI che elenca i comandi disponibili:

Comando	Funzione
dig	Raccogli l'output da dig per la risoluzione dei problemi DNS.
Esci	Torna al menu di configurazione.
h	Visualizza l'elenco dei comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete.

Comando	Funzione
	Note Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere della rete gateway.
ip	Mostra/manipola routing, dispositivi e tunnel. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere .
iptables	Strumento di amministrazione per il filtraggio dei IPv4 pacchetti e NAT.
tabelle ip6	Strumento di amministrazione per il filtraggio dei IPv6 pacchetti e NAT.
ncport	Verifica la connettività a una porta TCP specifica su una rete.
nping	Raccogli l'output da nping per la risoluzione dei problemi di rete.
open-support-channel	Connect to AWS Support.
save-iptables	Tabelle IP persistenti.

Comando	Funzione
save-routing-table	Salva la voce della tabella di routing appena aggiunta.
tcptraceroute	Raccogli l'output del traceroute sul traffico TCP verso una destinazione.

4. Dal prompt dei comandi della console del gateway, immettere il comando corrispondente alla funzione che si desidera utilizzare e seguire le istruzioni.

Per informazioni su un comando, digitate **`man`** + *`command name`* al prompt dei comandi.

Configurazione delle impostazioni di rete Amazon EC2 gateway

Puoi visualizzare e configurare le impostazioni di rete per Amazon EC2 File Gateway utilizzando la console locale del gateway.

Per configurare le impostazioni di rete

1. Accedi alla console locale sul tuo Amazon EC2 File Gateway. Per istruzioni, consulta Accesso alla console locale Amazon EC2 Gateway.
2. Dal menu principale AWS Appliance Activation - Configuration, inserisci il numero corrispondente per selezionare Network Configuration.
3. Dal menu Attivazione dell'AWS appliance - Configurazione di rete, immettete il numero corrispondente all'operazione che desiderate eseguire:
   - Modifica configurazione DNS: la console locale del gateway mostra gli adattatori disponibili per i server DNS primari e secondari. La console richiede quindi di fornire il nuovo indirizzo IP.
   - Visualizza la configurazione DNS: la console locale del gateway mostra gli adattatori disponibili per i server DNS primari e secondari.
   - Configura nome host: la console locale del gateway richiede di scegliere se il gateway utilizzerà un nome host statico specificato dall'utente o se acquisirà automaticamente un nome host tramite DCHP o rDNS.

> **Note**
>
> Se si sceglie di configurare un nome host statico per il gateway, è necessario creare un record A nel sistema DNS che punti l'indirizzo IP del gateway al relativo nome host statico.

- Visualizza la configurazione del nome host: la console locale del gateway mostra il nome host, la modalità di acquisizione, il dominio e il realm di Active Directory per Amazon File Gateway. EC2

Spegnimento della macchina virtuale gateway

Potrebbe essere necessario arrestare o riavviare la macchina virtuale per la manutenzione, ad esempio durante l'applicazione di una patch al tuo hypervisor. Chiudi il gateway locale VMs utilizzando l'interfaccia dell'hypervisor e le EC2 istanze Amazon utilizzando la console Amazon. EC2

> **Important**
>
> Se interrompi e avvii un EC2 gateway Amazon che utilizza lo storage temporaneo, il gateway sarà permanentemente offline. Questo accade perché il disco di storage fisico viene sostituito. Non esiste alcuna soluzione alternativa per questo problema. L'unica soluzione è eliminare il gateway e attivarne uno nuovo su una nuova istanza. EC2

Sostituzione del tuo S3 File Gateway esistente con una nuova istanza

Puoi sostituire un S3 File Gateway esistente con una nuova istanza man mano che le esigenze di dati e prestazioni aumentano o se ricevi una AWS notifica per la migrazione del gateway. Potrebbe essere necessario eseguire questa operazione se desideri spostare il gateway su una piattaforma host migliore o su EC2 istanze Amazon più recenti o aggiornare l'hardware del server sottostante.

La tabella seguente descrive i vantaggi e gli svantaggi di ciascun metodo. Utilizzando queste informazioni, selezionate il metodo più adatto all'ambiente gateway in uso, quindi fate riferimento ai passaggi della procedura nella sezione corrispondente riportata di seguito.

> **Note**
>
> Se è necessario accedere alla nuova console locale di Storage Gateway per completare uno dei due metodi, il nome utente iniziale è admin e la password temporanea è password.

> **Important**
>
> Utilizzare queste istruzioni solo per la migrazione delle appliance gateway che eseguono la versione 1.x. Non è possibile utilizzarle per migrare i dispositivi gateway che eseguono versioni precedenti.

	Metodo 1: migrazione del disco di cache e dell'ID gateway su un'istanza sostituti va*	Metodo 2: istanza sostitutiva con disco di cache vuoto e nuovo ID Gateway
Dati del disco di cache	I dati sul disco cache vengono conservati. Questo metodo è utile se il gateway dispone di un disco di cache di grandi dimensioni o se le applicazi oni sono sensibili al ritardo causato dalle operazioni di out-of-cache lettura.	I dati nella cache vengono scaricati dal AWS cloud. Questo metodo è ottimale per carichi di lavoro che richiedono molta scrittura, se le applicazioni sono in grado di tollerare il ritardo causato dalle letture. out-of-cache
Tempo di inattività	Il gateway rimarrà offline per 1-2 ore durante il processo di migrazione.	Le condivisioni di file sono sempre disponibili, ma i clienti sperimenteranno tempi di inattività brevi quando passeranno da una condivisi one di file all'altra durante la transizione alla nuova istanza.

	Metodo 1: migrazione del disco di cache e dell'ID gateway su un'istanza sostituti va*	Metodo 2: istanza sostitutiva con disco di cache vuoto e nuovo ID Gateway
		Note La scrittura su un bucket Amazon S3 da due condivisioni di file contempor aneamente non è supportata, quindi tutti i client devono essere rimappati da una condivisione all'altra contemporaneamente, anziché gradualmente.
ID gateway	Il nuovo gateway eredita il Gateway ID dal gateway che sostituisce.	Il gateway esistente e il gateway sostitutivo dispongon o di un gateway unico e separato. IDs

*Il metodo 1 è supportato solo durante la migrazione tra gateway con la stessa generazione e lo stesso numero di versione principale.

Note

La migrazione può essere eseguita solo tra gateway dello stesso tipo. Ad esempio, non è possibile migrare impostazioni o dati da un FSx File Gateway a un S3 File Gateway.

Metodo 1: migra il disco di cache e l'ID del gateway su un'istanza sostitutiva

Per migrare il disco di cache e l'ID Gateway di S3 FSx File Gateway su un'istanza sostitutiva:

1.
2. Utilizza i seguenti passaggi per aggiornare il gateway alla versione più recente

   a. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.

   b. Nel pannello di navigazione, scegli Gateway, quindi scegli il vecchio S3 File Gateway di cui desideri migrare.

   c. Fai clic su Aggiorna ora se disponibile. In caso contrario, il gateway utilizza già la versione più recente.
3. Verifica che la `CachePercentDirty` metrica nella scheda Monitoraggio per l'esistente S3 File Gateway Gateway sia. `0`
4. Spegni il S3 File Gateway Gateway esistente spegnendo la macchina virtuale (VM) host utilizzando i controlli dell'hypervisor.

   Per ulteriori informazioni sulla chiusura di un' EC2 istanza Amazon, consulta Stop and start your istance nella Amazon EC2 User Guide.

   Per ulteriori informazioni sullo spegnimento di una macchina virtuale KVM o Hyper-V VMware, consulta la documentazione dell'hypervisor.
5. Scollega tutti i dischi, inclusi il disco root e i dischi di cache, dalla vecchia macchina virtuale gateway.

   > **Note**
   >
   > Prendi nota dell'ID del volume del disco root e dell'ID del gateway associato a quel disco root. Sarà necessario scollegare questo disco dal nuovo hypervisor Storage Gateway in un passaggio successivo.

   Se utilizzi un' EC2 istanza Amazon come macchina virtuale per il tuo S3 File Gateway , consulta Scollegare un volume Amazon EBS da un'istanza Windows o Scollegare un volume Amazon EBS da un'istanza Linux nella Amazon User Guide. EC2

Per informazioni su come scollegare i dischi da una macchina virtuale KVM o Hyper-V VMware, consulta la documentazione del tuo hypervisor.

6. Crea una nuova istanza di macchina virtuale Gateway di archiviazione AWS hypervisor, ma non attivarla come gateway. In una fase successiva, questa nuova macchina virtuale assumerà l'identità del vecchio gateway.

   Per ulteriori informazioni sulla creazione di una nuova macchina virtuale hypervisor Storage Gateway, vedere Scelta di una piattaforma host e download della macchina virtuale.

   > **Note**
   >
   > Non aggiungere dischi di cache per la nuova macchina virtuale. Questa macchina virtuale utilizzerà gli stessi dischi di cache utilizzati dalla vecchia macchina virtuale.

7. Configura la tua nuova macchina virtuale Storage Gateway per utilizzare le stesse impostazioni di rete della vecchia macchina virtuale.

   L'impostazione predefinita per la configurazione di rete del gateway è DHCP (Dynamic Host Configuration Protocol). Con DHCP, al gateway viene assegnato automaticamente un indirizzo IP.

   Se è necessario configurare manualmente un indirizzo IP statico per la macchina virtuale gateway, vedere Configurazione dei parametri di rete.

   Se la macchina virtuale gateway deve utilizzare un proxy Socket Secure versione 5 (SOCKS5) per connettersi a Internet, vedere Routing del gateway distribuito tramite un proxy HTTP. EC2

8. Avvia la nuova VM Storage Gateway.

9. Collega i dischi scollegati dalla vecchia macchina virtuale gateway alla nuova macchina virtuale gateway. Non scollegare il disco root esistente dalla nuova macchina virtuale gateway.

   > **Note**
   >
   > Per migrare correttamente, tutti i dischi devono rimanere invariati. La modifica delle dimensioni del disco o di altri valori causa incongruenze nei metadati che impediscono il successo della migrazione.

10. Avvia il processo di migrazione del gateway connettendoti alla console locale della nuova macchina virtuale gateway o effettuando richieste Web all'indirizzo IP della macchina virtuale del nuovo gateway (descritto di seguito).

    a. Per utilizzare la console locale, seleziona l'opzione Migrate Gateway e fornisci l'ID del gateway esistente quando richiesto. Ti verrà richiesto di copiare le impostazioni applicate in precedenza sul vecchio gateway sul nuovo gateway. È possibile scegliere di applicarle o configurarle manualmente in un secondo momento. Vedere Accesso alla console locale del gateway.

    b. In alternativa, è possibile avviare il processo di migrazione del gateway connettendosi alla nuova macchina virtuale con un URL che utilizza il seguente formato.

    ```
    http://your-VM-IP-address/migrate?gatewayId=your-gateway-ID
    ```

    È possibile riutilizzare lo stesso indirizzo IP per la nuova macchina virtuale del gateway utilizzato per la vecchia macchina virtuale del gateway. L'URL si presenta in maniera simile al seguente esempio.

    ```
    http://198.51.100.123/migrate?gatewayId=sgw-12345678
    ```

    Utilizza questo URL da un browser o dalla riga di comando utilizzando `curl`, per avviare il processo di migrazione.

    Una volta completato correttamente il processo di migrazione del gateway, verrà visualizzato un messaggio di conferma dell'avvenuta migrazione.

11. Attendi che lo stato del gateway venga visualizzato come In esecuzione nella Gateway di archiviazione AWS console. A seconda della larghezza di banda disponibile, questa operazione può richiedere fino a 10 minuti.
12. Arresta la nuova VM Storage Gateway.
13. Scollega il disco principale del vecchio gateway, il cui ID di volume è stato annotato in precedenza, dal nuovo gateway.
14. Avvia la nuova VM Storage Gateway.
15. Se il gateway è stato aggiunto a un dominio Active Directory, ricongiungiti al dominio. Per istruzioni, consulta Utilizzo di Active Directory per autenticare gli utenti.

> **Note**
>
> È necessario completare questo passaggio anche se lo stato di S3 File Gateway appare come Unito.

16. Se il gateway utilizzava il metodo di autenticazione SMB Guest Access, la password dovrà essere reinserita. Per istruzioni, consulta Fornire agli ospiti l'accesso alla condivisione di file.
17. Verifica che le tue condivisioni siano disponibili all'indirizzo IP della nuova macchina virtuale gateway, quindi elimina la vecchia macchina virtuale gateway.

> **Warning**
>
> Un gateway eliminato non può più essere recuperato.

Per ulteriori informazioni sull'eliminazione di un' EC2 istanza Amazon, consulta Terminate your istance nella Amazon EC2 User Guide. Per ulteriori informazioni sull'eliminazione di una macchina virtuale KVM o Hyper-V VMware, consulta la documentazione del tuo hypervisor.

Metodo 2: istanza sostitutiva con disco di cache vuoto e nuovo Gateway ID

Per configurare un'istanza S3 File Gateway Gateway sostitutiva con un disco di cache vuoto e un nuovo ID Gateway:

1. Arresta tutte le applicazioni che stanno scrivendo sull'esistente S3 File Gateway Gateway. Verifica che la `CachePercentDirty` metrica nella scheda Monitoraggio sia quella indicata `0` prima di configurare le condivisioni di file sul nuovo gateway.
2. Utilizzate il pulsante AWS Command Line Interface (AWS CLI) per raccogliere e salvare le informazioni di configurazione relative al vostro S3 File Gateway File Gateway e alle condivisioni di file esistenti, procedendo come segue:

    a. Salvate le informazioni di configurazione del gateway per S3 File Gateway Gateway.

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Questo comando genera un blocco JSON che contiene metadati sul gateway, come il nome, le interfacce di rete, il fuso orario configurato e il relativo stato (se il gateway è in esecuzione).

b.

```
aws storagegateway describe-smb-settings --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Questo comando genera un blocco JSON che contiene metadati sulla condivisione di file SMB, ad esempio il nome di dominio, lo stato di Microsoft Active Directory, l'impostazione della password guest e il tipo di strategia di sicurezza.

c.

- Usa il seguente comando per le condivisioni di file SMB.

  ```
  aws storagegateway describe-smb-file-shares --file-share-arn-list
   "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
  ```

  Questo comando genera un blocco JSON che contiene metadati sulla condivisione di file SMB, come il nome, la classe di storage, lo stato, il ruolo IAM Amazon Resource Name (ARN), un elenco di client autorizzati ad accedere a S3 File Gateway FSx File Gateway di montaggio.

- Usa il comando seguente per le condivisioni di file NFS.

  ```
  aws storagegateway  describe-nfs-file-shares --file-share-arn-list
   "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
  ```

  Questo comando genera un blocco JSON che contiene metadati sulla condivisione di file NFS, come il nome, la classe di archiviazione, lo stato, l'ARN del ruolo IAM, un elenco di client autorizzati ad accedere a S3 File Gateway FSx File Gateway di montaggio.

3. Crea un nuovo S3 File Gateway FSx File Gateway . Se necessario, fai riferimento alle informazioni salvate nel passaggio 2.
4. Crea nuove condivisioni di file per il nuovo gateway con le stesse impostazioni e configurazioni delle condivisioni di file configurate sul vecchio gateway. Se necessario, fate riferimento alle informazioni salvate nel passaggio 2.
5. Verifica che il nuovo gateway funzioni correttamente, quindi rimappa/trasferisci i client dalle vecchie condivisioni di file alle nuove condivisioni di file nel modo più adatto al tuo ambiente.

6. Verifica che il nuovo gateway funzioni correttamente, quindi elimina il vecchio gateway dalla console Storage Gateway.

> **Important**
>
> Prima di eliminare un S3 File Gateway FSx , assicurati che non ci siano applicazioni attualmente in scrittura nella cache di quel gateway. L'eliminazione di un gateway in uso può comportare una perdita di dati.

> **Warning**
>
> Un gateway eliminato non può più essere recuperato.

7. Elimina la vecchia macchina virtuale gateway o l' EC2 istanza Amazon.

Eliminazione del gateway e rimozione delle risorse associate

Se non si intende continuare a utilizzarlo, un gateway può essere eliminato con le risorse a esso associate. La rimozione delle risorse non più utili consente di evitarne gli addebiti e quindi di ridurre la fattura mensile.

Quando si elimina un gateway, questo non viene più visualizzato nella console di Gateway di archiviazione AWS gestione e le relative connessioni al file system di condivisione vengono chiuse. Pur essendo la procedura di eliminazione uguale per tutti i tipi di gateway, per la rimozione delle risorse associate occorre seguire istruzioni specifiche, distinte in base al tipo di gateway da eliminare e all'host su cui è distribuito.

Puoi eliminare un gateway a livello di codice oppure utilizzando la console Storage Gateway. Seguono informazioni su come eliminare un gateway utilizzando la console Storage Gateway. Per eliminare un gateway in modo programmatico, consulta Documentazione di riferimento delle API Gateway di archiviazione AWS.

Eliminazione del gateway tramite la console Storage Gateway

La procedura di eliminazione è la stessa per tutti i tipi di gateway. Tuttavia, per rimuovere le risorse associate possono rendersi necessarie operazioni aggiuntive, distinte in base al tipo di gateway da

eliminare e all'host di distribuzione. Una volta rimosse, le risorse inutilizzate non comporteranno ulteriori costi.

> **Note**
>
> Per i gateway distribuiti su EC2 un'istanza Amazon, l'istanza continua a esistere finché non la elimini.
> Nel caso di gateway distribuiti su una macchina virtuale (VM), dopo l'eliminazione del gateway la VM resta disponibile nell'ambiente di virtualizzazione. Per rimuovere la macchina virtuale, utilizzare il client VMware vSphere, Microsoft Hyper-V Manager o il client Linux Kernel-based Virtual Machine (KVM) per connettersi all'host e rimuovere la macchina virtuale. Non è possibile riutilizzare la VM di un gateway eliminato per attivare un nuovo gateway.

Come eliminare un gateway

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi seleziona uno o più gateway da eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack). Viene visualizzata la finestra di dialogo di conferma.

   > **Warning**
   >
   > Prima di eseguire questa operazione, bisogna accertarsi che non vi siano applicazioni in fase di scrittura sui volumi del gateway. L'eliminazione di un gateway in uso può comportare una perdita di dati. Un gateway eliminato non può più essere recuperato.

4. Verifica di voler eliminare i gateway specificati, quindi digita la parola delete nella casella di conferma e scegli Elimina.
5. (Facoltativo) Se desideri fornire un feedback sul gateway eliminato, completa la finestra di dialogo di feedback, quindi scegli Invia. Altrimenti, seleziona Salta.

> **Important**
>
> Non pagherai più i costi del software dopo aver eliminato un gateway, ma risorse come il bucket Amazon S3 e le istanze Amazon EC2 persistono. Puoi rimuovere l' EC2istanza Amazon gateway dopo la rimozione del gateway di file. Se non hai bisogno dei dati nei bucket

Amazon S3 associati alle condivisioni di file, puoi scegliere di rimuovere i bucket Amazon S3. Per istruzioni, consulta Eliminazione del bucket.

Prestazioni e ottimizzazione

Questa sezione descrive linee guida e best practice per ottimizzare le prestazioni di File Gateway.

Argomenti

-
- Indicazioni sulle prestazioni per gateway con più condivisioni di file
- Massimizzazione del throughput di S3 File Gateway
- Ottimizzazione di S3 File Gateway per i backup dei database SQL Server

In questa sezione, puoi trovare linee guida per il provisioning dell'hardware per la tua macchina virtuale S3 File Gateway. Le configurazioni di istanza elencate nella tabella sono esempi e vengono fornite come riferimento.

Per prestazioni ottimali, la dimensione del disco della cache deve essere ottimizzata in base alle dimensioni del set di lavoro attivo. L'utilizzo di più dischi locali per la cache aumenta le prestazioni in scrittura parallelizzando l'accesso ai dati e comportando maggiori IOPS.

> **Note**
>
> Non è consigliabile utilizzare lo storage temporaneo. Per informazioni sull'utilizzo dello storage temporaneo, consulta Utilizzo dello storage temporaneo con i gateway EC2 .
> Per EC2 le istanze Amazon, se hai più di 5 milioni di oggetti nel tuo bucket S3 e utilizzi un volume SSD General Purpose, è necessario un volume root EBS minimo di 350 GiB per prestazioni accettabili del gateway durante l'avvio. Per informazioni su come aumentare le dimensioni del volume, consulta Modifica di un volume EBS utilizzando i volumi elastici (Console).
> Il limite di dimensione suggerito per le singole directory nei file system di condivisione di file collegati a è di 10.000 file per directory. È possibile utilizzare File Gateway con directory che contengono più di 10.000 file, ma le prestazioni potrebbero risentirne.

Nelle tabelle seguenti, le operazioni di lettura degli accessi alla cache sono letture dalle condivisioni di file fornite dalla cache. Le operazioni di mancata lettura della cache vengono lette dalle condivisioni di file fornite da Amazon S3.

Le tabelle seguenti mostrano esempi di configurazioni di S3 File Gateway.

Prestazioni di S3 File Gateway su client Linux

Configurazioni di esempio	Protocollo	Velocità effettiva di scrittura (dimensioni del file 1 GB)	Velocità effettiva di accessi alla cache	Velocità effettiva di mancata lettura della cache
Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: cache da 512 GiB, io1, 1.500 IOPS assegnati Prestazioni di rete minime: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protocollo NFS consigliato per Linux	NFSv3 - 1 thread	110 MiB/sec (0,92 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 thread	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	NFSv4 - 1 filo	130 MiB/sec (1,1 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)
	NFSv4 - 8 thread	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 filo	115 MiB/sec (1,0 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 thread	190 MiB/sec (1,6 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
Storage Gateway Hardware Appliance Prestazioni di rete minime: 10 Gbps	NFSv3 - 1 filo	265 MiB/sec (2,2 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 thread	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	NFSv4 - 1 filo	310 MiB/sec (2,6 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)

Configurazioni di esempio	Protocollo	Velocità effettiva di scrittura (dimensioni del file 1 GB)	Velocità effettiva di accessi alla cache	Velocità effettiva di mancata lettura della cache
	NFSv4 - 8 thread	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 filo	275 MiB/sec (2,4 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 thread	455 MiB/sec (3,8 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: 4 dischi cache NVME da 2 TB Prestazioni di rete minime: 10 Gbps Processore: 32 vCPU | RAM: 244 GB Protocollo NFS consigliato per Linux	NFSv3 - 1 thread	300 MiB/sec (2,5 Gbps)	590 MiB/sec (4,9 Gbps)	325 MiB/sec (2,7 Gbps)
	NFSv3 - 8 thread	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)
	NFSv4 - 1 filo	355 MiB/sec (3,0 Gbps)	590 MiB/sec (4,9 Gbps)	340 MiB/sec (2,9 Gbps)
	NFSv4 - 8 thread	575 MiB/sec (4,8 Gbps)	590 MiB/sec (4,9 Gbps)	575 MiB/sec (4,8 Gbps)
	SMBV3 - 1 filo	230 MiB/sec (1,9 Gbps)	325 MiB/sec (2,7 Gbps)	245 MiB/sec (2,0 Gbps)
	SMBV3 - 8 thread	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)

Prestazioni di File Gateway sui client Windows

Configurazioni di esempio	Protocollo	Velocità effettiva di scrittura (dimensioni del file 1 GB)	Velocità effettiva di accessi alla cache	Velocità effettiva di mancata lettura della cache
Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: cache da 512 GiB, io1, 1.500 IOPS assegnati Prestazioni di rete minime: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protocollo SMB consigliato per Windows	SMBV3 - 1 thread	150 MiB/sec (1,3 Gbps)	180 MiB/sec (1,5 Gbps)	20 MiB/sec (0,2 Gbps)
	SMBV3 - 8 thread	190 MiB/sec (1,6 Gbps)	335 MiB/sec (2,8 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 thread	95 MiB/sec (0,8 Gbps)	130 MiB/sec (1,1 Gbps)	20 MiB/sec (0,2 Gbps)
	NFSv3 - 8 thread	190 MiB/sec (1,6 Gbps)	330 MiB/sec (2,8 Gbps)	190 MiB/sec (1,6 Gbps)
Storage Gateway Hardware Appliance Prestazioni di rete minime: 10 Gbps	SMBV3 - 1 thread	230 MiB/sec (1,9 Gbps)	255 MiB/sec (2,1 Gbps)	20 MiB/sec (0,2 Gbps)
	SMBV3 - 8 thread	835 MiB/sec (7,0 Gbps)	475 MiB/sec (4,0 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 thread	135 MiB/sec (1,1 Gbps)	185 MiB/sec (1,6 Gbps)	20 MiB/sec (0,2 Gbps)
	NFSv3 - 8 thread	545 MiB/sec (4,6 Gbps)	470 MiB/sec (4,0 Gbps)	190 MiB/sec (1,6 Gbps)

Configurazioni di esempio	Protocollo	Velocità effettiva di scrittura (dimensioni del file 1 GB)	Velocità effettiva di accessi alla cache	Velocità effettiva di mancata lettura della cache
Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: 4 dischi cache NVME da 2 TB Prestazioni di rete minime: 10 Gbps Processore: 32 vCPU | RAM: 244 GB Protocollo SMB consigliato per Windows	SMBV3 - 1 thread	230 MiB/sec (1,9 Gbps)	265 MiB/sec (2,2 Gbps)	30 MiB/sec (0,3 Gbps)
	SMBV3 - 8 thread	835 MiB/sec (7,0 Gbps)	780 MiB/sec (6,5 Gbps)	250 MiB/sec (2,1 Gbps)
	NFSv3 - 1 filo	135 MiB/sec (1.1. Gbps)	220 MiB/sec (1,8 Gbps)	30 MiB/sec (0,3 Gbps)
	NFSv3 - 8 thread	545 MiB/sec (4,6 Gbps)	570 MiB/sec (4,8 Gbps)	240 MiB/sec (2,0 Gbps)

> **Note**
>
> Le prestazioni potrebbero variare in base alla configurazione della piattaforma host e alla larghezza di banda della rete. Le prestazioni di velocità effettiva di scrittura diminuiscono con la dimensione del file, con la velocità massima raggiungibile per file di piccole dimensioni (meno di 32 MiB) pari a 16 file al secondo.

Indicazioni sulle prestazioni per gateway con più condivisioni di file

Amazon S3 File Gateway supporta il collegamento di fino a 50 condivisioni di file a una singola appliance Storage Gateway. Aggiungendo più condivisioni di file per gateway, puoi supportare più utenti e carichi di lavoro gestendo al contempo un minor numero di gateway e risorse hardware

virtuali. Oltre ad altri fattori, il numero di condivisioni di file gestite da un gateway può influire sulle prestazioni di tale gateway. Questa sezione descrive come dovrebbero cambiare le prestazioni del gateway in base al numero di condivisioni di file allegate e consiglia configurazioni hardware virtuali per ottimizzare le prestazioni dei gateway che gestiscono più condivisioni.

In generale, l'aumento del numero di condivisioni di file gestite da un singolo Storage Gateway può avere le seguenti conseguenze:

- Maggiore tempo necessario per riavviare il gateway.
- Maggiore utilizzo di risorse hardware virtuali come vCPU e RAM.
- Riduzione delle prestazioni per le operazioni su dati e metadati in caso di saturazione delle risorse hardware virtuali.

La tabella seguente elenca le configurazioni hardware virtuali consigliate per i gateway che gestiscono più condivisioni di file:

Condivisioni di file per gateway	Impostazione della capacità del gateway consigliata	Core vCPU consigliati	RAM consigliata	Dimensione del disco principale consigliata			
1-10	Small	4 (tipo di EC2 istanza m4.xlarge o superiore)	16 GiB	80 GiB			
10-20	Media	8 (tipo di EC2 istanza m4.2xlarge o	32 GiB	160 GiB			

Condivisioni di file per gateway	Impostazione della capacità del gateway consigliata	Core vCPU consigliati	RAM consigliata	Dimensione del disco principale consigliata			
		superiore)					
20 o più	Large	16 (tipo di EC2 istanza m4.4xlarge o superiore)	64 GiB	240 GiB			

Oltre alle configurazioni hardware virtuali consigliate sopra, si consigliano le seguenti best practice per la configurazione e la manutenzione dei dispositivi Storage Gateway che gestiscono più condivisioni di file:

- Si consideri che la relazione tra il numero di condivisioni di file e la domanda posta sull'hardware virtuale del gateway non è necessariamente lineare. Alcune condivisioni di file potrebbero generare una maggiore velocità effettiva e quindi una maggiore richiesta di hardware rispetto ad altre. I consigli riportati nella tabella precedente si basano sulle capacità hardware massime e su vari livelli di velocità effettiva di condivisione dei file.
- Se ritieni che l'aggiunta di più condivisioni di file a un singolo gateway riduca le prestazioni, valuta la possibilità di spostare le condivisioni di file più attive su altri gateway. In particolare, se si utilizza una condivisione di file per un' very-high-throughputapplicazione, è consigliabile creare un gateway separato per tale condivisione di file.
- Non è consigliabile configurare un gateway per più applicazioni ad alto throughput e un altro per più applicazioni a basso throughput. Prova invece a distribuire le condivisioni di file ad alta e bassa velocità in modo uniforme tra i gateway per bilanciare la saturazione dell'hardware. Per misurare

la velocità effettiva di condivisione dei file, utilizza le metriche and. `ReadBytes` `WriteBytes` Per ulteriori informazioni, consulta Comprendere le metriche di condivisione dei file.

Massimizzazione del throughput di S3 File Gateway

Le sezioni seguenti descrivono le best practice per massimizzare il throughput tra i client NFS e SMB, S3 File Gateway e Amazon S3. Le indicazioni fornite in ogni sezione contribuiscono in modo incrementale a migliorare il throughput complessivo. Sebbene nessuna di queste raccomandazioni sia obbligatoria e non siano interdipendenti, sono state selezionate e ordinate in modo logico che consente di testare e ottimizzare le implementazioni Supporto di S3 File Gateway. Nell'implementare e testare questi suggerimenti, tieni presente che ogni implementazione di S3 File Gateway è unica, quindi i risultati possono variare.

S3 File Gateway fornisce un'interfaccia di file per archiviare e recuperare oggetti Amazon S3 utilizzando i protocolli di file NFS o SMB standard del settore, con una mappatura 1:1 nativa tra file e oggetto. Implementa S3 File Gateway come macchina virtuale in locale nel tuo ambiente KVM VMware Microsoft Hyper-V o Linux o nel cloud come istanza Amazon. AWS EC2 S3 File Gateway non è progettato per fungere da sostituto completo del NAS aziendale. S3 File Gateway emula un file system, ma non è un file system. L'utilizzo di Amazon S3 come storage backend durevole crea un sovraccarico aggiuntivo per ogni I/O operazione, quindi la valutazione delle prestazioni di S3 File Gateway rispetto a un NAS o un file server esistente non è un confronto equivalente.

Implementa il gateway nella stessa posizione dei tuoi client

Ti consigliamo di implementare l'appliance virtuale S3 File Gateway in una posizione fisica con la minore latenza di rete possibile tra l'appliance e i client NFS o SMB. Quando scegli una posizione per il gateway, considera quanto segue:

- Una latenza di rete inferiore rispetto al gateway può contribuire a migliorare le prestazioni dei client NFS o SMB.
- S3 File Gateway è progettato per tollerare una latenza di rete più elevata tra il gateway e Amazon S3 rispetto a quella tra il gateway e i client.
- Per le istanze S3 File Gateway distribuite in Amazon EC2, consigliamo di mantenere il gateway e i client NFS o SMB nello stesso gruppo di collocamento. Per ulteriori informazioni, consulta i gruppi di posizionamento per le tue EC2 istanze Amazon nella Amazon Elastic Compute Cloud User Guide.

Riduci i colli di bottiglia causati dai dischi lenti

Ti consigliamo di monitorare la `IoWaitPercent` CloudWatch metrica per identificare i rallentamenti nelle prestazioni che possono derivare dalla lentezza dei dischi di archiviazione sul tuo S3 File Gateway. Quando tenti di ottimizzare i problemi di prestazioni relativi al disco, considera quanto segue:

- `IoWaitPercent`riporta la percentuale di tempo in cui la CPU è in attesa di una risposta dai dischi root o cache.
- Quando `IoWaitPercent` è superiore al 5-10%, in genere indica un rallentamento delle prestazioni del gateway causato da dischi con prestazioni insufficienti. Questa metrica dovrebbe avvicinarsi il più possibile allo 0%, il che significa che il gateway non è mai in attesa sul disco, il che aiuta a ottimizzare le risorse della CPU.
- Puoi controllare `IoWaitPercent` nella scheda Monitoraggio della console Storage Gateway o configurare gli CloudWatch allarmi consigliati per avvisarti automaticamente se la metrica supera una soglia specifica. Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi consigliati per il gateway.
- Per ridurre al minimo i dischi root e cache del gateway, consigliamo di utilizzare uno NVMe o l'SSD. `IoWaitPercent`

Modifica l'allocazione delle risorse delle macchine virtuali per CPU, RAM e dischi cache

Quando si tenta di ottimizzare il throughput per S3 File Gateway, è importante allocare risorse sufficienti alla macchina virtuale del gateway, tra cui CPU, RAM e dischi di cache. I requisiti minimi di risorse virtuali di CPUs 4,16 GB di RAM e 150 GB di storage nella cache sono in genere adatti solo per carichi di lavoro più piccoli. Quando si allocano risorse virtuali per carichi di lavoro più grandi, si consiglia quanto segue:

- Aumenta il numero allocato tra 16 e 48, CPUs a seconda dell'utilizzo tipico della CPU generato da S3 File Gateway. Puoi monitorare l'utilizzo della CPU utilizzando la `UserCpuPercent` metrica. Per ulteriori informazioni, consulta Comprendere le metriche del gateway.
- Aumenta la RAM allocata tra 32 e 64 GB.

> **Note**
>
> S3 File Gateway non può utilizzare più di 64 GB di RAM.

- NVMe Utilizzate il nostro SSD per i dischi root e il disco di cache e dimensionate i dischi di cache in modo da allinearli al set di dati di picco che intendete scrivere sul gateway. Per ulteriori informazioni, consulta le best practice di dimensionamento della cache di S3 File Gateway sul canale ufficiale Amazon Web Services YouTube .
- Aggiungi almeno 4 dischi di cache virtuale al gateway, anziché utilizzare un unico disco di grandi dimensioni. Più dischi virtuali possono migliorare le prestazioni anche se condividono lo stesso disco fisico sottostante, ma i miglioramenti sono in genere maggiori quando i dischi virtuali si trovano su dischi fisici sottostanti diversi.

  Ad esempio, se desideri distribuire 12 TB di cache, puoi utilizzare una delle seguenti configurazioni:

  - 4 dischi cache da 3 TB
  - 8 dischi cache da 1,5 TB
  - 12 dischi cache da 1 TB

  Oltre alle prestazioni, ciò consente una gestione più efficiente della macchina virtuale nel tempo. Man mano che il carico di lavoro cambia, è possibile aumentare in modo incrementale il numero di dischi di cache e la capacità complessiva della cache, mantenendo al contempo le dimensioni originali di ogni singolo disco virtuale per preservare l'integrità del gateway.

  Per ulteriori informazioni, vedere Decidere la quantità di storage su disco locale.

Quando distribuisci S3 File Gateway come EC2 istanza Amazon, considera quanto segue:

- Il tipo di istanza scelto può influire in modo significativo sulle prestazioni del gateway. Amazon EC2 offre un'ampia flessibilità per regolare l'allocazione delle risorse per l'istanza S3 File Gateway.
- Per i tipi di EC2 istanze Amazon consigliati per S3 File Gateway, consulta Requisiti per i tipi di EC2 istanze Amazon.
- Puoi modificare il tipo di EC2 istanza Amazon che ospita un S3 File Gateway attivo. Ciò consente di regolare facilmente la generazione di EC2 hardware Amazon e l'allocazione delle risorse per trovare un price-to-performance rapporto ideale. Per modificare il tipo di istanza, utilizza la seguente procedura nella EC2 console Amazon:

  1. Arresta l' EC2 istanza Amazon.

2. Cambia il tipo di EC2 istanza Amazon.
3. Accendi l' EC2 istanza Amazon.

> **Note**
>
> L'arresto di un'istanza che ospita un S3 File Gateway interromperà temporaneamente l'accesso alla condivisione dei file. Assicurati di pianificare una finestra di manutenzione, se necessario.

- Il price-to-performance rapporto di un' EC2 istanza Amazon si riferisce alla potenza di calcolo ottenuta al prezzo pagato. In genere, EC2 le istanze Amazon di nuova generazione offrono il price-to-performance rapporto migliore, con hardware più recente e prestazioni migliorate a un costo relativamente inferiore rispetto alle generazioni precedenti. Fattori come il tipo di istanza, la regione e i modelli di utilizzo influiscono su questo rapporto, quindi è importante selezionare l'istanza giusta per il carico di lavoro specifico per ottimizzare il rapporto costo/efficacia.

Regola il livello di sicurezza delle PMI

Il SMBv3 protocollo consente sia la firma SMB che la crittografia SMB, con alcuni compromessi in termini di prestazioni e sicurezza. Per ottimizzare il throughput, è possibile regolare il livello di sicurezza SMB del gateway per specificare quali di queste funzionalità di sicurezza vengono applicate alle connessioni client. Per ulteriori informazioni, consulta Impostare un livello di sicurezza per il gateway.

Quando regolate il livello di sicurezza SMB, tenete presente quanto segue:

- Il livello di sicurezza predefinito per S3 File Gateway è Enforce encryption. Questa impostazione applica sia la crittografia che la firma per le connessioni client SMB alle condivisioni di file del gateway, il che significa che tutto il traffico dal client al gateway è crittografato. Questa impostazione non influisce sul traffico dal gateway a AWS, che è sempre crittografato.

  Il gateway limita ogni connessione client crittografata a una singola vCPU. Ad esempio, se si dispone di un solo client crittografato, tale client sarà limitato a una sola vCPU, anche se 4 o più v CPUs sono allocate al gateway. Per questo motivo, la velocità effettiva per le connessioni crittografate da un singolo client a S3 File Gateway è in genere limitata tra 40-60 MB/s.
- Se i requisiti di sicurezza consentono un approccio più rilassato, è possibile modificare il livello di sicurezza impostandolo su Client negotiated, che disabiliterà la crittografia SMB e applicherà solo

la firma SMB. Con questa impostazione, le connessioni client al gateway possono utilizzare più v, il che in genere si traduce in un aumento delle CPUs prestazioni di throughput.

> **Note**
>
> Dopo aver modificato il livello di sicurezza SMB per S3 File Gateway, è necessario attendere che lo stato della condivisione dei file passi da Aggiornamento a Disponibile nella console Storage Gateway, quindi disconnettere e ricollegare i client SMB affinché la nuova impostazione abbia effetto.

Utilizza più thread e client per parallelizzare le operazioni di scrittura

È difficile ottenere le massime prestazioni di throughput con un S3 File Gateway che utilizza un solo client NFS o SMB per scrivere un file alla volta, perché la scrittura sequenziale da un singolo client è un'operazione a thread singolo. Consigliamo invece di utilizzare più thread di ogni client NFS o SMB per scrivere più file in parallelo e di utilizzare più client NFS o SMB contemporaneamente sul tuo S3 File Gateway per massimizzare il throughput del gateway.

L'utilizzo di più thread può migliorare significativamente le prestazioni. Tuttavia, l'utilizzo di più thread richiede più risorse di sistema, il che può influire negativamente sulle prestazioni se il gateway non è dimensionato per soddisfare l'aumento del carico. In un'implementazione tipica, ci si può aspettare di ottenere migliori prestazioni di throughput aggiungendo più thread e client, fino a raggiungere i limiti massimi di hardware e larghezza di banda per il gateway. Ti consigliamo di sperimentare diversi numeri di thread per trovare l'equilibrio ottimale tra velocità e utilizzo delle risorse di sistema per la tua specifica configurazione hardware e di rete.

Considerate le seguenti informazioni sugli strumenti più comuni che possono aiutarvi a testare la configurazione del thread e del client:

- Puoi testare le prestazioni di scrittura multithread utilizzando strumenti come robocopy per copiare un set di file in una condivisione di file sul tuo gateway. Per impostazione predefinita, robocopy utilizza 8 thread per copiare i file, ma è possibile specificare fino a 128 thread.

  Per usare più thread con robocopy, aggiungi lo `/MT:n` switch al tuo comando, n dov'è il numero di thread che vuoi usare. Per esempio:

  ```
  robocopy C:\source D:\destination /MT:64
  ```

Questo comando utilizzerà 64 thread per l'operazione di copia.

> **Note**
>
> Si sconsiglia di utilizzare Windows Explorer per trascinare e rilasciare i file durante il test della velocità effettiva massima, poiché questo metodo è limitato a un singolo thread e copia i file in sequenza.

Per ulteriori informazioni, consulta robocopy sul sito Web Microsoft Learn.

- Puoi anche eseguire test utilizzando strumenti comuni di benchmarking dello storage come DISKSPD o FIO. Questi strumenti offrono opzioni per regolare il numero di thread, la profondità di I/O e altri parametri in base ai requisiti specifici del carico di lavoro.

  DiskSpd consente di controllare il numero di thread utilizzando il parametro. `-t` Per esempio:

  ```
  diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
  ```

  Questo comando di esempio esegue le seguenti operazioni:

  - Crea un file di test da 10 GB () `-c1G`
  - Funziona per 300 secondi () `-d300`
  - Esegue un I/O test casuale con il 50% di letture e 50% di scrittura () `-r -w50`
  - Utilizza 64 thread () `-t64`
  - Imposta la profondità della coda a 32 per thread () `-o32`
  - Utilizza una dimensione del blocco di 1 MB () `-b1M`
  - Disattiva la memorizzazione nella cache hardware e software () `-h -L`

  Per ulteriori informazioni, consulta Utilizzare DISKSPD per testare le prestazioni di archiviazione del carico di lavoro sul sito Web Microsoft Learn.

- FIO utilizza il `numjobs` parametro per controllare il numero di thread paralleli. Per esempio:

  ```
  fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
  --size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
  group_reporting
  ```

  Questo comando di esempio esegue le seguenti operazioni:

- Esegue un I/O test casuale (`--rw=randrw`)
- Esegue il 70% di letture e il 30% di scrittura () `--rwmixread=70`
- Utilizza una dimensione del blocco di 1 MB () `--bs=1M`
- Imposta la I/O profondità su 64 () `--iodepth=64`
- Test su un file da 10 GB (`--size=10G`)
- Funziona per 5 minuti (`--runtime=300`)
- Crea 64 lavori paralleli (thread) (`--numjobs=64`)
- Utilizza un motore asincrono I/O () `--ioengine=libaio`
- Raggruppa i risultati per un'analisi più semplice () `--group_reporting`

  Per ulteriori informazioni, consultate la pagina man di fio Linux.
-

Disattiva l'aggiornamento automatico della cache

La funzionalità di aggiornamento automatico della cache consente a S3 File Gateway di aggiornare automaticamente i metadati, il che può aiutare a catturare eventuali modifiche apportate da utenti o applicazioni al set di file scrivendo direttamente nel bucket Amazon S3, anziché tramite il gateway. Per ulteriori informazioni, consulta Refreshing Amazon S3 bucket Object Cache.

Per ottimizzare il throughput del gateway, consigliamo di disattivare questa funzionalità nelle distribuzioni in cui tutte le letture e le scritture sul bucket Amazon S3 verranno eseguite tramite il tuo S3 File Gateway.

Quando configuri l'aggiornamento automatico della cache, considera quanto segue:

- Se devi utilizzare l'aggiornamento automatico della cache perché gli utenti o le applicazioni della tua distribuzione scrivono occasionalmente direttamente su Amazon S3, ti consigliamo di configurare l'intervallo di tempo più lungo possibile tra gli aggiornamenti, in modo che sia comunque pratico per le tue esigenze aziendali. Un intervallo di aggiornamento della cache più lungo aiuta a ridurre il numero di operazioni sui metadati che il gateway deve eseguire durante la navigazione nelle directory o la modifica dei file.

  Ad esempio: imposta l'aggiornamento automatico della cache su 24 ore, anziché 5 minuti, se ciò è tollerabile per il carico di lavoro.
- L'intervallo di tempo minimo è di 5 minuti. L'intervallo massimo è di 30 giorni.

- Se scegli di impostare un intervallo di aggiornamento della cache molto breve, ti consigliamo di testare l'esperienza di navigazione nelle directory per i tuoi client NFS e SMB. Il tempo necessario per aggiornare la cache del gateway può aumentare notevolmente a seconda del numero di file e sottodirectory nel bucket Amazon S3.

Aumenta il numero di thread di caricamento di Amazon S3

Per impostazione predefinita, S3 File Gateway apre 8 thread per il caricamento dei dati di Amazon S3, che fornisce una capacità di caricamento sufficiente per le distribuzioni più comuni. Tuttavia, è possibile che un gateway riceva dati dai client NFS e SMB a una velocità superiore a quella che può caricare su Amazon S3 con la capacità standard di 8 thread, il che può far sì che la cache locale raggiunga il limite di archiviazione.

In circostanze specifiche, Supporto puoi aumentare il numero di thread di caricamento di Amazon S3 per il tuo gateway da 8 a 40, il che consente di caricare più dati in parallelo. A seconda della larghezza di banda e di altri fattori specifici della distribuzione, ciò può aumentare significativamente le prestazioni di caricamento e contribuire a ridurre la quantità di storage nella cache necessaria per supportare il carico di lavoro.

Ti consigliamo di utilizzare la `CachePercentDirty` CloudWatch metrica per monitorare la quantità di dati archiviati sui dischi di cache del gateway locale che non sono ancora stati caricati su Amazon S3 e di Supporto contattarci per determinare se l'aumento del numero del pool di thread di caricamento possa migliorare il throughput per il tuo S3 File Gateway. Per ulteriori informazioni, consulta Understanding gateway metrics.

> **Note**
>
> Questa impostazione consuma risorse aggiuntive della CPU del gateway. Si consiglia di monitorare l'utilizzo della CPU del gateway e di aumentare le risorse CPU allocate, se necessario.

Aumenta le impostazioni di timeout SMB

Quando S3 File Gateway copia file di grandi dimensioni in una condivisione di file SMB, la connessione client SMB può scadere dopo un periodo di tempo prolungato.

Consigliamo di estendere l'impostazione del timeout della sessione SMB per i client SMB a 20 minuti o più, a seconda della dimensione dei file e della velocità di scrittura del gateway. L'impostazione predefinita è 300 secondi o 5 minuti. Per ulteriori informazioni, vedi Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway.

Attiva il blocco opportunistico per le applicazioni compatibili

Il blocco opportunistico, o «oplocks», è abilitato di default per ogni nuovo S3 File Gateway. Quando si utilizzano oplock con applicazioni compatibili, il client raggruppa più operazioni più piccole in operazioni più grandi, il che è più efficiente per il client, il gateway e la rete. Ti consigliamo di mantenere attivo il blocco opportunistico se utilizzi applicazioni che sfruttano la memorizzazione nella cache locale lato client, come Microsoft Office, Adobe Suite e molte altre, perché può migliorare significativamente le prestazioni.

Se disattivi il blocco opportunistico, le applicazioni che supportano gli oplock in genere aprono file di grandi dimensioni (50 MB o più) molto più lentamente. Questo ritardo si verifica perché il gateway invia i dati in parti da 4 KB, il che si traduce in una velocità effettiva elevata I/O e bassa.

Regola la capacità del gateway in base alla dimensione del set di file di lavoro

Il parametro di capacità del gateway specifica il numero massimo di file per i quali il gateway memorizzerà i metadati nella cache locale. Per impostazione predefinita, la capacità del gateway è impostata su Small, il che significa che il gateway archivia i metadati per un massimo di 5 milioni di file. L'impostazione predefinita funziona bene per la maggior parte dei carichi di lavoro, anche se ci sono centinaia di milioni o addirittura miliardi di oggetti in Amazon S3, perché in una distribuzione tipica si accede attivamente solo a un piccolo sottoinsieme di file alla volta. Questo gruppo di file viene definito «set di lavoro».

Se il carico di lavoro accede regolarmente a un set di lavoro superiore a 5 milioni di file, il gateway dovrà eliminare frequentemente la cache, ossia piccole operazioni di I/O archiviate nella RAM e mantenute sul disco principale. Ciò può influire negativamente sulle prestazioni del gateway poiché il gateway recupera nuovi dati da Amazon S3.

Puoi monitorare la `IndexEvictions` metrica per determinare il numero di file i cui metadati sono stati rimossi dalla cache per fare spazio a nuove voci. Per ulteriori informazioni, consulta Understanding gateway metrics.

Si consiglia di utilizzare l'azione `UpdateGatewayInformation` API per aumentare la capacità del gateway in modo che corrisponda al numero di file del set di lavoro tipico. Per ulteriori informazioni, consulta UpdateGatewayInformation.

> **Note**
>
> L'aumento della capacità del gateway richiede RAM e capacità del disco root aggiuntive.
>
> - Le dimensioni ridotte (5 milioni di file) richiedono almeno 16 GB di RAM e 80 GB di disco root.
> - Medium (10 milioni di file) richiede almeno 32 GB di RAM e 160 GB di disco root.
> - Le dimensioni grandi (20 milioni di file) richiedono 64 GB di RAM e 240 GB di disco root.

> **Important**
>
> La capacità del gateway non può essere ridotta.

Implementa più gateway per carichi di lavoro più grandi

Quando possibile, consigliamo di suddividere il carico di lavoro su più gateway, anziché consolidare molte condivisioni di file su un unico gateway di grandi dimensioni. Ad esempio, è possibile isolare una condivisione di file molto utilizzata su un gateway, raggruppando le condivisioni di file utilizzate meno frequentemente su un altro gateway.

Quando pianifichi una distribuzione con più gateway e condivisioni di file, considera quanto segue:

- Il numero massimo di condivisioni di file su un singolo gateway è 50, ma il numero di condivisioni di file gestite da un gateway può influire sulle prestazioni del gateway. Per ulteriori informazioni, consulta Guida alle prestazioni per gateway con più condivisioni di file.
- Le risorse su ogni S3 File Gateway sono condivise tra tutte le condivisioni di file, senza partizionamento.
- Una singola condivisione di file con un utilizzo intenso può influire sulle prestazioni di altre condivisioni di file sul gateway.

> **Note**
>
> Non è consigliabile creare più condivisioni di file mappate sulla stessa posizione Amazon S3 da più gateway, a meno che almeno una di esse non sia di sola lettura.
> Le scritture simultanee sullo stesso file da più gateway sono considerate uno scenario di scrittura multipla, che può causare problemi di integrità dei dati.

Ottimizzazione di S3 File Gateway per i backup dei database SQL Server

I backup dei database sono un caso d'uso comune e consigliato per S3 File Gateway, che offre una conservazione conveniente a breve e lungo termine archiviando i backup del database in Amazon S3, con la possibilità di eseguire il ciclo di vita su livelli di storage più bassi, se necessario. Con questa soluzione, puoi ridurre la necessità di applicazioni di backup aziendali utilizzando strumenti integrati come SQL Server Management Studio e Oracle RMAN.

Le sezioni seguenti descrivono le migliori pratiche per ottimizzare l'implementazione di S3 File Gateway per prestazioni ottimizzate e un supporto conveniente per centinaia di terabyte di backup di database SQL. Le linee guida fornite in ogni sezione contribuiscono in modo incrementale a migliorare il throughput complessivo. Sebbene nessuna di queste raccomandazioni sia obbligatoria e non siano interdipendenti, sono state selezionate e ordinate in modo logico che consente di testare e ottimizzare le implementazioni Supporto di S3 File Gateway. Nell'implementare e testare questi suggerimenti, tieni presente che ogni implementazione di S3 File Gateway è unica, quindi i risultati possono variare.

S3 File Gateway fornisce un'interfaccia di file per archiviare e recuperare oggetti Amazon S3 utilizzando i protocolli di file NFS o SMB standard del settore, con una mappatura 1:1 nativa tra file e oggetto. Implementa S3 File Gateway come macchina virtuale in locale nel tuo ambiente KVM VMware Microsoft Hyper-V o Linux o nel cloud come istanza Amazon. AWS EC2 S3 File Gateway non è progettato per fungere da sostituto completo del NAS aziendale. S3 File Gateway emula un file system, ma non è un file system. L'utilizzo di Amazon S3 come storage backend durevole crea un sovraccarico aggiuntivo per ogni I/O operazione, quindi la valutazione delle prestazioni di S3 File Gateway rispetto a un NAS o un file server esistente non è un confronto equivalente.

Implementa il gateway nella stessa posizione dei server SQL

Ti consigliamo di implementare l'appliance virtuale S3 File Gateway in una posizione fisica con la minore latenza di rete possibile tra l'appliance e i server SQL. Quando scegli una posizione per il gateway, considera quanto segue:

- Una latenza di rete inferiore rispetto al gateway può contribuire a migliorare le prestazioni dei client SMB, come i server SQL.
- S3 File Gateway è progettato per tollerare una latenza di rete più elevata tra il gateway e Amazon S3 rispetto a quella tra il gateway e i client.
- Per le istanze S3 File Gateway distribuite in Amazon EC2, consigliamo di mantenere il gateway e i server SQL nello stesso gruppo di collocamento. Per ulteriori informazioni, consulta i gruppi di posizionamento per le tue EC2 istanze Amazon nella Amazon Elastic Compute Cloud User Guide.

Riduci i colli di bottiglia causati dai dischi lenti

Ti consigliamo di monitorare la `IoWaitPercent` CloudWatch metrica per identificare i rallentamenti nelle prestazioni che possono derivare dalla lentezza dei dischi di archiviazione sul tuo S3 File Gateway. Quando tenti di ottimizzare i problemi di prestazioni relativi al disco, considera quanto segue:

- `IoWaitPercent`riporta la percentuale di tempo in cui la CPU è in attesa di una risposta dai dischi root o cache.
- Quando `IoWaitPercent` è superiore al 5-10%, in genere indica un rallentamento delle prestazioni del gateway causato da dischi con prestazioni insufficienti. Questa metrica dovrebbe avvicinarsi il più possibile allo 0%, il che significa che il gateway non è mai in attesa sul disco, il che aiuta a ottimizzare le risorse della CPU.
- Puoi controllare `IoWaitPercent` nella scheda Monitoraggio della console Storage Gateway o configurare gli CloudWatch allarmi consigliati per avvisarti automaticamente se la metrica supera una soglia specifica. Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi consigliati per il gateway.
- Per ridurre al minimo i dischi root e cache del gateway, consigliamo di utilizzare uno NVMe o l'SSD. `IoWaitPercent`

Regola l'allocazione delle risorse della macchina virtuale S3 File Gateway per CPU, RAM e dischi cache

Quando si tenta di ottimizzare il throughput per S3 File Gateway, è importante allocare risorse sufficienti alla macchina virtuale del gateway, tra cui CPU, RAM e dischi di cache. I requisiti minimi di risorse virtuali di CPUs 4,16 GB di RAM e 150 GB di storage nella cache sono in genere adatti solo per carichi di lavoro più piccoli. Quando si allocano risorse virtuali per carichi di lavoro più grandi, si consiglia quanto segue:

- Aumenta il numero allocato tra 16 e 48, CPUs a seconda dell'utilizzo tipico della CPU generato da S3 File Gateway. Puoi monitorare l'utilizzo della CPU utilizzando la `UserCpuPercent` metrica. Per ulteriori informazioni, consulta Comprendere le metriche del gateway.
- Aumenta la RAM allocata tra 32 e 64 GB.

> **Note**
>
> S3 File Gateway non può utilizzare più di 64 GB di RAM.

- NVMe Utilizzate il nostro SSD per i dischi root e il disco di cache e dimensionate i dischi di cache in modo da allinearli al set di dati di picco che intendete scrivere sul gateway. Per ulteriori informazioni, consulta le best practice di dimensionamento della cache di S3 File Gateway sul canale ufficiale Amazon Web Services YouTube .
- Aggiungi almeno 4 dischi di cache virtuale al gateway, anziché utilizzare un unico disco di grandi dimensioni. Più dischi virtuali possono migliorare le prestazioni anche se condividono lo stesso disco fisico sottostante, ma i miglioramenti sono in genere maggiori quando i dischi virtuali si trovano su dischi fisici sottostanti diversi.

  Ad esempio, se desideri distribuire 12 TB di cache, puoi utilizzare una delle seguenti configurazioni:

  - 4 dischi cache da 3 TB
  - 8 dischi cache da 1,5 TB
  - 12 dischi cache da 1 TB

  Oltre alle prestazioni, ciò consente una gestione più efficiente della macchina virtuale nel tempo. Man mano che il carico di lavoro cambia, è possibile aumentare in modo incrementale il numero di dischi di cache e la capacità complessiva della cache, mantenendo al contempo le dimensioni originali di ogni singolo disco virtuale per preservare l'integrità del gateway.

Per ulteriori informazioni, vedere Decidere la quantità di storage su disco locale.

Quando distribuisci S3 File Gateway come EC2 istanza Amazon, considera quanto segue:

- Il tipo di istanza scelto può influire in modo significativo sulle prestazioni del gateway. Amazon EC2 offre un'ampia flessibilità per regolare l'allocazione delle risorse per l'istanza S3 File Gateway.
- Per i tipi di EC2 istanze Amazon consigliati per S3 File Gateway, consulta Requisiti per i tipi di EC2 istanze Amazon.
- Puoi modificare il tipo di EC2 istanza Amazon che ospita un S3 File Gateway attivo. Ciò consente di regolare facilmente la generazione di EC2 hardware Amazon e l'allocazione delle risorse per trovare un price-to-performance rapporto ideale. Per modificare il tipo di istanza, utilizza la seguente procedura nella EC2 console Amazon:
  1. Arresta l' EC2 istanza Amazon.
  2. Cambia il tipo di EC2 istanza Amazon.
  3. Accendi l' EC2 istanza Amazon.

  > **Note**
  >
  > L'arresto di un'istanza che ospita un S3 File Gateway interromperà temporaneamente l'accesso alla condivisione dei file. Assicurati di pianificare una finestra di manutenzione, se necessario.
- Il price-to-performance rapporto di un' EC2 istanza Amazon si riferisce alla potenza di calcolo ottenuta al prezzo pagato. In genere, EC2 le istanze Amazon di nuova generazione offrono il price-to-performance rapporto migliore, con hardware più recente e prestazioni migliorate a un costo relativamente inferiore rispetto alle generazioni precedenti. Fattori come il tipo di istanza, la regione e i modelli di utilizzo influiscono su questo rapporto, quindi è importante selezionare l'istanza giusta per il carico di lavoro specifico per ottimizzare il rapporto costo/efficacia.

Migliora la produttività dei client SMB regolando il livello di sicurezza del tuo S3 File Gateway

Il SMBv3 protocollo consente sia la firma SMB che la crittografia SMB, con alcuni compromessi in termini di prestazioni e sicurezza. Per ottimizzare il throughput, è possibile regolare il livello di sicurezza SMB del gateway per specificare quali di queste funzionalità di sicurezza vengono

applicate alle connessioni client. Per ulteriori informazioni, consulta Impostare un livello di sicurezza per il gateway.

Quando regolate il livello di sicurezza SMB, tenete presente quanto segue:

- Il livello di sicurezza predefinito per S3 File Gateway è Enforce encryption. Questa impostazione applica sia la crittografia che la firma per le connessioni client SMB alle condivisioni di file del gateway, il che significa che tutto il traffico dal client al gateway è crittografato. Questa impostazione non influisce sul traffico dal gateway a AWS, che è sempre crittografato.

  Il gateway limita ogni connessione client crittografata a una singola vCPU. Ad esempio, se si dispone di un solo client crittografato, tale client sarà limitato a una sola vCPU, anche se 4 o più v CPUs sono allocate al gateway. Per questo motivo, la velocità effettiva per le connessioni crittografate da un singolo client a S3 File Gateway è in genere limitata tra 40-60 MB/s.
- Se i requisiti di sicurezza consentono un approccio più rilassato, è possibile modificare il livello di sicurezza impostandolo su Client negotiated, che disabiliterà la crittografia SMB e applicherà solo la firma SMB. Con questa impostazione, le connessioni client al gateway possono utilizzare più v, il che in genere si traduce in un aumento delle CPUs prestazioni di throughput.

> **Note**
>
> Dopo aver modificato il livello di sicurezza SMB per S3 File Gateway, è necessario attendere che lo stato della condivisione dei file passi da Aggiornamento a Disponibile nella console Storage Gateway, quindi disconnettere e ricollegare i client SMB affinché la nuova impostazione abbia effetto.

Migliora la produttività dei client SMB suddividendo i backup SQL in più file

- È difficile ottenere le massime prestazioni di throughput con un S3 File Gateway: solo un server SQL scrive un file alla volta, perché la scrittura sequenziale da un singolo server SQL è un'operazione a thread singolo. Si consiglia invece di utilizzare più thread da ciascun server SQL per scrivere più file in parallelo e di utilizzare più server SQL contemporaneamente su S3 File Gateway per massimizzare il throughput del gateway. Con i backup SQL, la suddivisione dei backup in più file consente a ciascun file di utilizzare un thread separato, che scriverà più file contemporaneamente nella condivisione di file S3 File Gateway. Più thread hai, maggiore è la velocità effettiva che puoi raggiungere, fino ai limiti del gateway.

- SQL Server supporta la scrittura su più file contemporaneamente durante una singola operazione di backup. Ad esempio, è possibile specificare più destinazioni di file utilizzando i comandi T-SQL o SQL Server Management Studio (SSMS). Ogni file utilizza un thread separato per inviare dati dal server SQL alla condivisione di file del gateway. Questo approccio consente una migliore I/O velocità di trasmissione, che può migliorare in modo significativo la velocità e l'efficienza del backup.

Quando configuri i backup del server SQL, considera quanto segue:

- Suddividendo i backup in più file, gli amministratori di SQL Server possono ottimizzare i tempi di backup e gestire i backup di database di grandi dimensioni in modo più efficace.
- Il numero di file utilizzati dipende dalla configurazione dello storage e dai requisiti prestazionali del server. Per i database di grandi dimensioni, si consiglia di suddividere i backup in diversi file più piccoli tra 10 GB e 20 GB ciascuno.
- Non esiste un limite rigoroso al numero di file su cui SQL Server può scrivere durante un backup, ma considerazioni pratiche come l'architettura di archiviazione e la larghezza di banda della rete dovrebbero guidare questa scelta.

Per ulteriori informazioni, consultare:

- Esegui il backup di SQL Server il 43-67% più velocemente scrivendo su più file
- Archivia facilmente i tuoi backup di SQL Server in Amazon S3 utilizzando File Gateway

Previeni errori di copia di file di grandi dimensioni aumentando le impostazioni di timeout SMB

Quando S3 File Gateway copia file di backup SQL di grandi dimensioni in una condivisione di file SMB, la connessione client SMB può scadere dopo un periodo di tempo prolungato. Consigliamo di estendere l'impostazione del timeout della sessione SMB per i client SMB di SQL Server a 20 minuti o più, a seconda delle dimensioni dei file e della velocità di scrittura del gateway. L'impostazione predefinita è 300 secondi o 5 minuti. Per ulteriori informazioni, vedi Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway.

Aumenta il numero di thread di caricamento di Amazon S3

Per impostazione predefinita, S3 File Gateway apre 8 thread per il caricamento dei dati di Amazon S3, che fornisce una capacità di caricamento sufficiente per le distribuzioni più comuni. Tuttavia, è possibile che un gateway riceva dati dai server SQL a una velocità superiore a quella che può caricare su Amazon S3 con la capacità standard di 8 thread, il che può far sì che la cache locale raggiunga il limite di archiviazione.

In circostanze specifiche, Supporto puoi aumentare il numero di thread di caricamento di Amazon S3 per il tuo gateway da 8 a 40, il che consente di caricare più dati in parallelo. A seconda della larghezza di banda e di altri fattori specifici della distribuzione, ciò può aumentare significativamente le prestazioni di caricamento e contribuire a ridurre la quantità di storage nella cache necessaria per supportare il carico di lavoro.

Ti consigliamo di utilizzare la `CachePercentDirty` CloudWatch metrica per monitorare la quantità di dati archiviati sui dischi di cache del gateway locale che non sono ancora stati caricati su Amazon S3 e di Supporto contattarci per determinare se l'aumento del numero del pool di thread di caricamento possa migliorare il throughput per il tuo S3 File Gateway. Per ulteriori informazioni, consulta Understanding gateway metrics.

> **Note**
>
> Questa impostazione consuma risorse aggiuntive della CPU del gateway. Si consiglia di monitorare l'utilizzo della CPU del gateway e di aumentare le risorse CPU allocate, se necessario.

Disattiva l'aggiornamento automatico della cache

La funzionalità di aggiornamento automatico della cache consente a S3 File Gateway di aggiornare automaticamente i metadati, il che può aiutare a catturare eventuali modifiche apportate da utenti o applicazioni al set di file scrivendo direttamente nel bucket Amazon S3, anziché tramite il gateway. Per ulteriori informazioni, consulta Refreshing Amazon S3 bucket Object Cache.

Per ottimizzare il throughput del gateway, consigliamo di disattivare questa funzionalità nelle distribuzioni in cui tutte le letture e le scritture sul bucket Amazon S3 verranno eseguite tramite il tuo S3 File Gateway.

Quando configuri l'aggiornamento automatico della cache, considera quanto segue:

- Se devi utilizzare l'aggiornamento automatico della cache perché gli utenti o le applicazioni della tua distribuzione scrivono occasionalmente direttamente su Amazon S3, ti consigliamo di configurare l'intervallo di tempo più lungo possibile tra gli aggiornamenti, in modo che sia comunque pratico per le tue esigenze aziendali. Un intervallo di aggiornamento della cache più lungo aiuta a ridurre il numero di operazioni sui metadati che il gateway deve eseguire durante la navigazione nelle directory o la modifica dei file.

  Ad esempio: imposta l'aggiornamento automatico della cache su 24 ore, anziché 5 minuti, se ciò è tollerabile per il carico di lavoro.
- L'intervallo di tempo minimo è di 5 minuti. L'intervallo massimo è di 30 giorni.
- Se scegli di impostare un intervallo di aggiornamento della cache molto breve, ti consigliamo di testare l'esperienza di navigazione nelle directory per i tuoi server SQL. Il tempo necessario per aggiornare la cache del gateway può aumentare notevolmente a seconda del numero di file e sottodirectory nel bucket Amazon S3.

Implementa più gateway per supportare il carico di lavoro

Storage Gateway può supportare backup SQL per ambienti di grandi dimensioni con centinaia di database SQL, più SQL Server e centinaia di terabyte di dati di backup suddividendo il carico di lavoro su più gateway.

Quando pianifichi una distribuzione con più gateway e server SQL, considera quanto segue:

- Un singolo gateway può in genere caricare fino a 20 TB al giorno, con risorse hardware e larghezza di banda sufficienti. Puoi aumentare questo limite fino a 40 TB al giorno aumentando il numero di thread di caricamento di Amazon S3.
- Ti consigliamo di eseguire un proof-of-concept test per misurare le prestazioni e tenere conto di tutte le variabili della distribuzione. Dopo aver determinato il throughput di picco del carico di lavoro di backup SQL, puoi scalare il numero di gateway per soddisfare i tuoi requisiti.
- Consigliamo di progettare la soluzione pensando alla crescita, poiché il numero di database e le dimensioni dei database possono aumentare nel tempo. Per continuare a scalare e supportare un carico di lavoro crescente, puoi implementare gateway aggiuntivi in base alle esigenze.

Risorse aggiuntive per i carichi di lavoro di backup del database

- Archivia i backup di SQL Server in Amazon S3 utilizzando Gateway di archiviazione AWS

- Archivia facilmente i tuoi backup di SQL Server in Amazon S3 utilizzando File Gateway
- Utilizzo Gateway di archiviazione AWS per archiviare i backup dei database Oracle in Amazon S3
- Backup dei database Oracle su Amazon S3 su larga scala
- Integra un database SAP ASE in Amazon S3 utilizzando Gateway di archiviazione AWS
- Come viene utilizzato One AWS Hero Gateway di archiviazione AWS per il backup nel cloud
- Migliori pratiche per il dimensionamento della cache di S3 File Gateway

Sicurezza nello AWS Storage Gateway

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Storage Gateway, vedere AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la responsabilità dell'utente è determinata dal AWS servizio utilizzato. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si usa Storage Gateway. Gli argomenti seguenti illustrano come configurare Storage Gateway per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse dello Storage Gateway.

Protezione dei dati in AWS Storage Gateway

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Storage Gateway. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal

modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando si lavora con Storage Gateway o altro Servizi AWS utilizzando la console AWS CLI, l'API o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati utilizzando AWS KMS

Storage Gateway utilizza SSL/TLS (Secure Layers/Transport Socket Layer Security) per crittografare i dati trasferiti tra l'appliance gateway e AWS lo storage. Per impostazione predefinita, Storage Gateway utilizza le chiavi di crittografia gestite da Amazon S3 (SSE-S3) per crittografare sul lato server tutti i dati archiviati in Amazon S3. Puoi utilizzare l'API Storage Gateway per configurare il gateway per crittografare i dati archiviati nel cloud utilizzando la crittografia lato server con le chiavi AWS Key Management Service (SSE-KMS).

Crittografia di una condivisione file

Puoi configurare le condivisioni di file su S3 File Gateway per crittografare gli oggetti archiviati con chiavi AWS KMS gestite utilizzando SSE-KMS o DSSE-KMS. Per informazioni sui metodi di crittografia supportati per la condivisione di file, consulta Crittografare gli oggetti archiviati da File Gateway in Amazon S3.

Quando lo utilizzi AWS KMS per crittografare i tuoi dati, tieni presente quanto segue:

- I dati vengono crittografati nel cloud mentre sono inattivi.
- Gli utenti IAM devono disporre delle autorizzazioni necessarie per chiamare le operazioni AWS KMS API. Per ulteriori informazioni, consulta Utilizzo delle policy IAM con AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

> **Important**
>
> Quando usi una AWS KMS chiave per la crittografia lato server, devi scegliere una chiave simmetrica. Storage Gateway non supporta le chiavi asimmetriche. Per ulteriori informazioni, consulta Utilizzo di chiavi simmetriche e asimmetriche nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni su AWS KMS, consulta Cos'è? AWS Key Management Service

Gestione delle identità e degli accessi per AWS Storage Gateway

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse SGW. AWS IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso tramite policy
- Come funziona AWS Storage Gateway con IAM
- Esempi di policy basate su identità per AWS Storage Gateway

- Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway
- Utilizzo dei tag per controllare l'accesso al gateway e alle risorse
- Utilizzo di Windows ACLs per limitare l'accesso alla condivisione di file SMB

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona AWS Storage Gateway con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate su identità per AWS Storage Gateway)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso federato degli utenti, le autorizzazioni utente IAM temporanee, l'accesso tra account, l'accesso tra servizi e le applicazioni in esecuzione su Amazon. EC2 Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o risorse. AWS Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste

politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona AWS Storage Gateway con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS SGW, scopri quali funzionalità IAM sono disponibili per l'uso con AWS SGW.

Funzionalità IAM che puoi utilizzare con AWS Storage Gateway

Funzionalità IAM	AWS Supporto SGW
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì

Funzionalità IAM	AWS Supporto SGW
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come AWS SGW e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per SGW AWS

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per SGW AWS

Per visualizzare esempi di politiche basate sull'identità di AWS SGW, vedere. Esempi di policy basate su identità per AWS Storage Gateway

Politiche basate sulle risorse all'interno di SGW AWS

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per SGW AWS

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni AWS SGW, vedere Actions Defined by AWS Storage Gateway nel Service Authorization Reference.

Le azioni politiche in AWS SGW utilizzano il seguente prefisso prima dell'azione:

```
sgw
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "sgw:action1",
```

```
      "sgw:action2"
         ]
```

Per visualizzare esempi di politiche basate sull'identità di AWS SGW, vedere. Esempi di policy basate su identità per AWS Storage Gateway

Risorse politiche per SGW AWS

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse AWS SGW e relativi ARNs, vedere Resources Defined by AWS Storage Gateway nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, vedere Azioni definite da AWS Storage Gateway.

Per visualizzare esempi di politiche AWS SGW basate sull'identità, vedere. Esempi di policy basate su identità per AWS Storage Gateway

Chiavi relative alle condizioni delle politiche per SGW AWS

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio

uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione AWS SGW, vedere Condition Keys for AWS Storage Gateway nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, vedere Azioni definite da AWS Storage Gateway.

Per visualizzare esempi di politiche AWS SGW basate sull'identità, vedere. Esempi di policy basate su identità per AWS Storage Gateway

ACLs AWS in SGW

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con SGW AWS

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con SGW AWS

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Sessioni di accesso diretto per SGW AWS

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale chiamante e Servizio AWS, in combinazione con la richiesta, di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AWS SGW

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità SGW. AWS Modificate i ruoli di servizio solo quando AWS SGW fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per SGW AWS

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono

visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate su identità per AWS Storage Gateway

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare AWS risorse SGW. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per i dettagli sulle azioni e sui tipi di risorse definiti da AWS SGW, incluso il formato di ARNs per ogni tipo di risorsa, vedere Actions, Resources and Condition Keys for AWS Storage Gateway nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console SGW AWS
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS risorse SGW nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti

specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console SGW AWS

Per accedere alla console AWS Storage Gateway, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli sulle risorse AWS SGW presenti nel proprio. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console AWS SGW, collega anche la AWS SGW *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per maggiori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway

Utilizzate le seguenti informazioni per aiutarvi a diagnosticare e risolvere i problemi più comuni che potreste riscontrare quando lavorate con AWS SGW e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in SGW AWS
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AWS SGW

Non sono autorizzato a eseguire un'azione in SGW AWS

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `sgw:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `sgw:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a AWS SGW.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS SGW. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

> **Important**
>
> Storage Gateway può assumere ruoli di servizio esistenti che vengono passati utilizzando l'azione delle `iam:PassRole` policy, ma non supporta le policy IAM che utilizzano la chiave di `iam:PassedToService` contesto per limitare l'azione a servizi specifici.
> Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS Identity and Access Management :
>
> - IAM: passa un ruolo IAM a un AWS servizio specifico
> - Concessione a un utente delle autorizzazioni per trasferire un ruolo a un servizio AWS
> - Chiavi disponibili per IAM

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AWS SGW

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS SGW supporta queste funzionalità, consulta. Come funziona AWS Storage Gateway con IAM
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Utilizzo dei tag per controllare l'accesso al gateway e alle risorse

Per controllare l'accesso alle risorse e alle azioni del gateway, puoi utilizzare policy AWS Identity and Access Management (IAM) basate su tag. È possibile fornire il controllo in due modi:

1. Controllare l'accesso alle risorse di gateway in base ai tag di queste risorse.
2. Controllare quali tag possono essere trasferiti in una condizione di richiesta IAM.

Per informazioni su come usare i tag per controllare l'accesso, consulta Controllo degli accessi tramite tag.

Controllo dell'accesso in base ai tag di una risorsa

Per controllare le operazioni che un utente o un ruolo può eseguire su una risorsa di gateway, è possibile usare i tag sulla risorsa. Ad esempio, è possibile consentire o negare operazioni API specifiche su una risorsa di gateway di file in base alla coppia chiave-valore del tag sulla risorsa.

L'esempio seguente consente a un utente o un ruolo di eseguire le operazioni `ListTagsForResource`, `ListFileShares` e `DescribeNFSFileShares` su tutte le risorse. La policy si applica solo se il tag nella risorsa ha la chiave impostata su `allowListAndDescribe` e il valore impostato su `yes`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
}
```

Controllo dell'accesso in base ai tag in una richiesta IAM

Per controllare cosa può fare un utente su una risorsa gateway, puoi utilizzare le condizioni di una policy IAM basata sui tag. Ad esempio, puoi scrivere una policy che consenta o neghi a un utente la possibilità di eseguire operazioni API specifiche in base al tag fornito al momento della creazione della risorsa.

In questo esempio, la prima istruzione consente all'utente di creare un gateway solo se la coppia chiave-valore del tag fornito al momento della creazione del gateway è **`Department`** e **`Finance`**. Quando si utilizza l'operazione API, si aggiunge questo tag alla richiesta di attivazione.

La seconda istruzione consente all'utente di creare una condivisione file NFS (Network File System) o Server Message Block (SMB) su un gateway solo se la coppia chiave-valore del tag sul gateway corrisponde a **`Department`**e **`Finance`**. Inoltre, l'utente deve aggiungere un tag alla condivisione file e la coppia chiave-valore del tag deve essere **`Department`** e **`Finance`**. Puoi aggiungere i tag a una condivisione file nel momento in cui la crei. Non ci sono autorizzazioni per le operazioni `AddTagsToResource` o `RemoveTagsFromResource`, quindi l'utente non è in grado di eseguire queste operazioni sul gateway o sulla condivisione file.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
```

```
            ],
            "Resource":"*",
            "Condition":{
               "StringEquals":{
                  "aws:ResourceTag/Department":"Finance",
                  "aws:RequestTag/Department":"Finance"
               }
            }
         }
      ]
}
```

Utilizzo di Windows ACLs per limitare l'accesso alla condivisione di file SMB

Amazon S3 file gateway supporta due metodi diversi per controllare l'accesso a file e directory archiviati tramite una condivisione di file SMB: autorizzazioni POSIX o Windows. ACLs

Questa sezione descrive come utilizzare gli elenchi di controllo degli accessi di Microsoft Windows (ACLs) sulle condivisioni di file SMB che utilizzano Microsoft Active Directory (AD) per l'autenticazione. Utilizzando Windows ACLs, è possibile impostare autorizzazioni dettagliate su file e cartelle nella condivisione di file SMB.

Di seguito sono riportate alcune caratteristiche importanti di Windows sulle condivisioni di file SMB ACLs :

- Windows ACLs viene selezionato per impostazione predefinita per le condivisioni di file SMB quando il gateway di file viene aggiunto a un dominio Active Directory.
- Quando ACLs sono attivate, le informazioni ACL vengono mantenute nei metadati degli oggetti Amazon S3.
- Il gateway ne conserva fino a 10 ACLs per file o cartella.
- Quando utilizzi una condivisione di file SMB ACLs attivata per accedere agli oggetti S3 creati all'esterno del gateway, gli oggetti ACLs ereditano le informazioni dalla cartella principale.

> **Note**
>
> La lista di controllo degli accessi root predefinita per un file di condivisione SMB offre accesso completo a tutti, ma è possibile modificare le autorizzazioni della ACL root. Puoi usare root ACLs per controllare l'accesso alla condivisione di file. È possibile impostare chi può montare

la condivisione di file (mappare l'unità) e quali autorizzazioni ottiene l'utente per i file e le cartelle in modo ricorsivo nella condivisione di file. Tuttavia, consigliamo di impostare questa autorizzazione nella cartella di livello superiore nel bucket S3 in modo che la lista di controllo degli accessi venga mantenuta.

È possibile attivare Windows ACLs quando si crea una nuova condivisione di file SMB utilizzando l'operazione Create SMBFile Share API. Oppure puoi attivare Windows ACLs su una condivisione di file SMB esistente utilizzando l'operazione API Update SMBFile Share.

Attivazione di Windows ACLs su una nuova condivisione di file SMB

Segui i passaggi seguenti per attivare Windows ACLs su una nuova condivisione di file SMB.

Per attivare Windows ACLs durante la creazione di una nuova condivisione di file SMB

1. Creare un file gateway se non si dispone già di uno. Per ulteriori informazioni, consulta Crea il tuo gateway.
2. Se il gateway non è stato aggiunto a un dominio, aggiungerlo a un dominio. Per ulteriori informazioni, vedere Utilizzo di Active Directory per autenticare gli utenti.
3. Creare una condivisione di file SMB. Per ulteriori informazioni, consultare la pagina
4. Attiva Windows ACLs sulla condivisione di file dalla console Storage Gateway.

   Per utilizzare la console Storage Gateway, effettuare le seguenti operazioni:

   a. Scegliere la condivisione file e scegliere Edit file share (Modifica condivisione file).
   b. Per l'opzione File/directory access controlled by (Accesso a file/directory controllato da) scegliere Windows Access Control List (Lista di controllo accessi di Windows).
5. (Facoltativo) Aggiungere un utente amministratore a AdminUsersList, se si desidera che l'utente amministratore abbia i privilegi di aggiornamento ACLs su tutti i file e le cartelle della condivisione di file.

> **Note**
>
> Se hai configurato gli elenchi Utenti e gruppi consentiti e negati nelle impostazioni della condivisione di file SMB, non ACLs concederai alcun accesso che sostituisca tali elenchi. Gli elenchi Utenti e gruppi consentiti e negati vengono valutati in precedenza ACLs e controllano quali utenti possono montare o accedere alla condivisione di file. Se alcuni

utenti o gruppi vengono inseriti nell'elenco Consentito, l'elenco viene considerato attivo e solo tali utenti possono montare la condivisione di file.
Dopo che un utente ha installato una condivisione di file ACLs , offri una protezione più granulare che controlli a quali file o cartelle specifici l'utente può accedere.

6. Aggiorna il file ACLs per le cartelle principali nella cartella principale. A tale scopo, utilizzate Windows File Explorer per configurare le ACLs cartelle nella condivisione di file SMB.

   > **Note**
   >
   > Se configuri ACLs nella cartella principale anziché nella cartella principale sotto root, le autorizzazioni ACL non vengono mantenute in Amazon S3.

   Ti consigliamo di eseguire l'impostazione ACLs nella cartella di primo livello sotto la radice della condivisione di file, anziché impostarla ACLs direttamente nella cartella principale della condivisione di file. Questo approccio mantiene le informazioni come metadati di oggetti in Amazon S3.

7. Attiva l'ereditarietà in base alle esigenze.

   > **Note**
   >
   > Puoi attivare l'ereditarietà per le condivisioni di file create dopo l'8 maggio 2019.

Se attivi l'ereditarietà e aggiorni le autorizzazioni in modo ricorsivo, Storage Gateway aggiorna tutti gli oggetti nel bucket S3. A seconda del numero di oggetti nel bucket, l'aggiornamento può richiedere alcuni minuti per il completamento.

Attivazione di Windows su una condivisione di file SMB esistente ACLs

Segui i passaggi seguenti per attivare Windows ACLs su una condivisione di file SMB esistente con autorizzazioni POSIX.

Per attivare Windows ACLs su una condivisione di file SMB esistente utilizzando la console Storage Gateway

1. Scegliere la condivisione file e scegliere Edit file share (Modifica condivisione file).

2. Per l'opzione File/directory access controlled by (Accesso a file/directory controllato da) scegliere Windows Access Control List (Lista di controllo accessi di Windows).
3. Attiva l'ereditarietà in base alle esigenze.

> **Note**
>
> Non è consigliabile impostarlo ACLs a livello root, perché se si esegue questa operazione e si elimina il gateway, è necessario reimpostarlo nuovamente. ACLs

Se attivi l'ereditarietà e aggiorni le autorizzazioni in modo ricorsivo, Storage Gateway aggiorna tutti gli oggetti nel bucket S3. A seconda del numero di oggetti nel bucket, l'aggiornamento può richiedere alcuni minuti per il completamento.

Limitazioni nell'utilizzo di Windows ACLs

Tieni presenti le seguenti limitazioni quando usi Windows ACLs per controllare l'accesso alle condivisioni di file SMB:

- Windows ACLs è supportato solo nelle condivisioni di file che utilizzano Active Directory per l'autenticazione quando si utilizzano client Windows SMB per accedere alle condivisioni di file.
- I gateway di file supportano un massimo di 10 voci ACL per ogni file e directory.
- I gateway di file non supportano le `Alarm` voci `Audit` e, che sono voci della lista di controllo degli accessi di sistema (SACL). I gateway di file supportano le `Deny` voci `Allow` e le voci, che sono voci della lista di controllo di accesso discrezionale (DACL).
- I file gateway non supportano le autorizzazioni Advanced Access Control Entry (ACE).
- Le impostazioni ACL root di condivisione dei file SMB sono presenti solo sul gateway e le impostazioni vengono mantenute in aggiornamenti e riavvii del gateway.

> **Note**
>
> Se configuri ACLs nella cartella principale anziché nella cartella principale sotto la cartella principale, le autorizzazioni ACL non vengono mantenute in Amazon S3.

In tali condizioni, assicurati di eseguire quanto segue:

- Se configuri più gateway per accedere allo stesso bucket Amazon S3, configura l'ACL root su ciascuno dei gateway per mantenere coerenti le autorizzazioni.
- Se elimini una condivisione di file e la ricrei sullo stesso bucket Amazon S3, assicurati di utilizzare lo stesso set di root. ACLs

Convalida della conformità per AWS Storage Gateway

I revisori di terze parti valutano la sicurezza e la conformità di AWS Storage Gateway nell'ambito di più programmi di AWS conformità. Questi includono SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR e HITRUST CSF.

Per informazioni generali, vedere Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La responsabilità per la conformità quando utilizzi Storage Gateway è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. AWS fornisce le risorse seguenti per semplificare la conformità:

- Guide rapide su sicurezza e conformità Guide introduttive implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi all'HIPAA. AWS
- AWS Risorse per la conformità Risorse per la conformità: questa raccolta di potrebbe riguardare il settore e la località in cui operate.
- Valutazione delle risorse in base alle regole contenute nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub CSPM— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente di verificare la conformità agli standard e alle best practice del settore della sicurezza. AWS

Resilienza nello AWS Storage Gateway

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità.

An Regione AWS è un luogo fisico in tutto il mondo in cui i data center sono raggruppati. Ogni gruppo di data center logici è denominato zona di disponibilità (AZ). Ciascuno Regione AWS è composto da un minimo di tre isolati e fisicamente separati AZs all'interno di un'area geografica. A differenza di altri provider di servizi cloud, che spesso definiscono una regione come un unico data center, il design multiplo di AZ di ognuno Regione AWS offre vantaggi distinti. Ogni AZ dispone di alimentazione, raffreddamento e sicurezza fisica indipendenti ed è connessa tramite reti ridondanti ultra-low-latency. Se l'implementazione richiede un'attenzione particolare all'elevata disponibilità, è possibile configurare servizi e risorse in modo multiplo per ottenere una maggiore tolleranza AZs ai guasti.

Regioni AWS soddisfano i massimi livelli di sicurezza, conformità e protezione dei dati dell'infrastruttura. Tutto il traffico intercorrente AZs è crittografato. Le prestazioni di rete sono sufficienti per eseguire la replica sincrona tra. AZs AZs semplificano il partizionamento di servizi e risorse per un'elevata disponibilità. Se la distribuzione è partizionata AZs, le risorse sono meglio isolate e protette da problemi come interruzioni di corrente, fulmini, tornado, terremoti e altro ancora. AZs sono fisicamente separate da una distanza significativa da qualsiasi altra AZ, sebbene si trovino tutte nel raggio di 100 km (60 miglia) l'una dall'altra.

Per ulteriori informazioni sulle zone Regioni AWS di disponibilità, vedere AWS Global Infrastructure.

Oltre all'infrastruttura AWS globale, Storage Gateway supporta VMware vSphere High Availability (VMware HA) per proteggere i carichi di lavoro di storage da guasti hardware, hypervisor o di rete. Per ulteriori informazioni, vedere Using VMware vSphere High Availability with Storage Gateway.

Sicurezza dell'infrastruttura in AWS Storage Gateway

In quanto servizio gestito, AWS Storage Gateway è protetto dalle procedure di sicurezza di rete AWS globali descritte in Security Pillar - AWS Well-Architected Framework.

Si utilizzano chiamate API AWS pubblicate per accedere a Storage Gateway attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.2. I client devono, inoltre, supportare le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

> **Note**
>
> È necessario trattare l'appliance AWS Storage Gateway come una macchina virtuale gestita e non tentare di accedere o modificare in alcun modo la sua installazione. Il tentativo di installare il software di scansione o di aggiornare qualsiasi pacchetto software utilizzando metodi diversi dal normale meccanismo di aggiornamento del gateway può causare il malfunzionamento del gateway e influire sulla nostra capacità di supportare o correggere il gateway.
>
> AWS esamina, analizza e corregge CVEs regolarmente. Le correzioni di questi problemi sono incluse in Storage Gateway come parte del normale ciclo di rilascio del software. Queste correzioni vengono in genere applicate come parte del normale processo di aggiornamento del gateway durante le finestre di manutenzione programmata. Per ulteriori informazioni sugli aggiornamenti del gateway, vedere Gestione degli aggiornamenti del gateway tramite la Gateway di archiviazione AWS console .

AWS Migliori pratiche di sicurezza

AWS fornisce una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste pratiche potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni. Per ulteriori informazioni, consulta Best practice di sicurezza AWS.

Registrazione e monitoraggio Gateway di archiviazione AWS

Storage Gateway è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Storage Gateway. CloudTrail acquisisce tutte le chiamate API per Storage Gateway come eventi. Le chiamate acquisite includono le chiamate dalla console di Storage Gateway e le chiamate di codice alle operazioni delle API Storage Gateway. Se crei un trail, puoi attivare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Storage Gateway. Se non configuri un percorso, puoi comunque visualizzare gli eventi

più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Storage Gateway, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni sullo Storage Gateway in CloudTrail

CloudTrail viene attivato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Storage Gateway, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nel proprio AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Storage Gateway, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le operazioni di Storage Gateway sono registrate e documentate nell'argomento Operazioni. Ad esempio, le chiamate a `ActivateGatewayListGateways`, e `ShutdownGateway` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).

- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di registro di Storage Gateway

Un trail è una configurazione che consente la consegna di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'azione.

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
```

```
                                                    "responseElements": {
                                                                          "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                                    },
                                                    "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                                    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                                    "eventType": "AwsApiCall",
                                                    "apiVersion": "20130630",
                                                    "recipientAccountId": "444455556666"
            }]
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l' ListGatewaysazione.

```
{
 "Records": [{
              "eventVersion": "1.02",
              "userIdentity": {
                               "type": "IAMUser",
                               "principalId": "AIDAII5AUEPBH2M7JTNVC",
                               "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                               "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                               " userName ":" JohnDoe "
                               },

                               " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                               " eventSource ":" storagegateway.amazonaws.com ",
                               " eventName ":" ListGateways ",
                               " awsRegion ":" us-east-2 ",
                               " sourceIPAddress ":" 192.0.2.0 ",
                               " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                               " requestParameters ":null,
                               " responseElements ":null,
                               "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                               " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                               " eventType ":" AwsApiCall ",
```

```
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
            }]
}
```

Risoluzione dei problemi relativi all'implementazione dello Storage Gateway

Di seguito, puoi trovare informazioni sulle migliori pratiche e sulla risoluzione dei problemi relativi a gateway, piattaforme host, condivisioni di file, alta disponibilità, ripristino dei dati e sicurezza. Le informazioni sulla risoluzione dei problemi dei gateway locali riguardano i gateway distribuiti sulle piattaforme di virtualizzazione supportate. Le informazioni sulla risoluzione dei problemi di alta disponibilità riguardano i gateway in esecuzione sulla piattaforma VMware vSphere High Availability (HA).

Argomenti

- Risoluzione dei problemi: problemi relativi al gateway offline- Scopri come diagnosticare i problemi che possono far apparire il gateway offline nella console Storage Gateway.
- Risoluzione dei problemi: problemi relativi ad Active Directory- Scopri cosa fare se ricevi messaggi di errore come `NETWORK_ERRORTIMEOUT`, o `ACCESS_DENIED` quando tenti di aggiungere File Gateway a un dominio Microsoft Active Directory.
- Risoluzione dei problemi: problemi di attivazione del gateway- Scopri cosa fare se ricevi un messaggio di errore interno quando tenti di attivare lo Storage Gateway.
- Risoluzione dei problemi: problemi relativi al gateway locale- Scopri i problemi tipici che potresti riscontrare lavorando con i gateway locali e come consentire la connessione al gateway Supporto per facilitare la risoluzione dei problemi.
- Risoluzione dei problemi: problemi di configurazione di Microsoft Hyper-V- Scopri i problemi tipici che potresti riscontrare durante l'implementazione di Storage Gateway sulla piattaforma Microsoft Hyper-V.
- Risoluzione dei problemi: problemi relativi al EC2 gateway Amazon- Trova informazioni sui problemi tipici che potresti riscontrare quando lavori con i gateway distribuiti su Amazon. EC2
- Risoluzione dei problemi: problemi relativi alle apparecchiature hardware- Scopri come risolvere i problemi che potresti riscontrare con l'appliance hardware AWS Storage Gateway.
- Risoluzione dei problemi: problemi relativi a File Gateway- Trova informazioni che possano aiutarti a comprendere la causa degli errori e delle notifiche di integrità che appaiono nei CloudWatch log di File Gateway.
- Risoluzione dei problemi: problemi relativi alla condivisione dei file- Scopri le azioni che puoi intraprendere in caso di problemi imprevisti con la condivisione di file.

- Risoluzione dei problemi: problemi di elevata disponibilità- Scopri cosa fare in caso di problemi con i gateway distribuiti in un ambiente VMware HA.

Risoluzione dei problemi: gateway offline nella console Storage Gateway

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se la Gateway di archiviazione AWS console mostra che il gateway è offline.

Il gateway potrebbe essere visualizzato come offline per uno o più dei seguenti motivi:

- Il gateway non può raggiungere gli endpoint del servizio Storage Gateway.
- Il gateway si è spento in modo imprevisto.
- Un disco di cache associato al gateway è stato disconnesso o modificato oppure è guasto.

Per riportare il gateway online, identificate e risolvete il problema che ha causato la disconnessione del gateway.

Controlla il firewall o il proxy associato

Se hai configurato il gateway per utilizzare un proxy o hai posizionato il gateway protetto da un firewall, consulta le regole di accesso del proxy o del firewall. Il proxy o il firewall devono consentire il traffico da e verso le porte di rete e gli endpoint di servizio richiesti da Storage Gateway. Per ulteriori informazioni, vedere Requisiti di rete e firewall Requisiti di .

Verifica la presenza di un'ispezione continua tramite SSL o deep packet del traffico del tuo gateway

Se è attualmente in corso un'ispezione SSL o deep-packet sul traffico di rete tra il gateway e il gateway AWS, il gateway potrebbe non essere in grado di comunicare con gli endpoint di servizio richiesti. Per riportare il gateway online, è necessario disattivare l'ispezione.

Controlla la metrica IOWait Percentuale dopo un riavvio o un aggiornamento del software

Dopo un riavvio o un aggiornamento del software, controlla se la `IOWaitPercent` metrica per File Gateway è 10 o superiore. Ciò potrebbe rallentare la risposta del gateway durante la ricostruzione

della cache dell'indice in RAM. Per ulteriori informazioni, consulta Risoluzione dei problemi: utilizzo delle metriche Risoluzione dei : utilizzo CloudWatch delle metriche. CloudWatch

Verificare la presenza di un'interruzione dell'alimentazione o di un guasto hardware sull'host dell'hypervisor

Un'interruzione dell'alimentazione o un guasto hardware sull'host hypervisor del gateway può causare lo spegnimento imprevisto del gateway e renderlo irraggiungibile. Dopo aver ripristinato l'alimentazione e la connettività di rete, il gateway sarà nuovamente raggiungibile.

Dopo che il gateway sarà tornato online, assicurati di adottare le misure necessarie per ripristinare i dati. Per ulteriori informazioni, consulta Best practice: recovery your data .

Verifica la presenza di problemi con un disco di cache associato

Il gateway può andare offline se almeno uno dei dischi di cache associati al gateway è stato rimosso, modificato o ridimensionato o se è danneggiato.

Se un disco cache funzionante è stato rimosso dall'host dell'hypervisor:

1. Arresta il gateway.
2. Aggiungere nuovamente il disco.

   > **Note**
   >
   > Assicurati di aggiungere il disco allo stesso nodo del disco.

3. Riavviare il gateway.

Se un disco cache è danneggiato, è stato sostituito o è stato ridimensionato:

- Segui la procedura del Metodo 2 descritta in Sostituzione del tuo S3 File Gateway esistente con una nuova istanza per configurare un nuovo gateway e scaricare nuovamente le informazioni sul disco di cache dal cloud. AWS

Risoluzione dei problemi: problemi di connessione del gateway ad Active Directory

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se ricevi messaggi di errore come `NETWORK_ERRORTIMEOUT`, o `ACCESS_DENIED` quando tenti di aggiungere File Gateway a un dominio Microsoft Active Directory.

Per risolvere questi errori, esegui i controlli e le configurazioni seguenti.

Verifica che il gateway possa raggiungere il controller di dominio eseguendo un test nping

Per eseguire un test nping:

1. Connect alla console locale del gateway utilizzando il software di gestione dell'hypervisor (VMwareHyper-V o KVM) per i gateway locali o utilizzando ssh per i gateway Amazon. EC2
2. Inserisci il numero corrispondente per selezionare Gateway Console, quindi inserisci per elencare tutti i comandi disponibili. h Per testare la connettività tra la macchina virtuale Storage Gateway e il dominio, eseguire il comando seguente:

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > `corp.domain.com`Sostituiscilo con il nome DNS del dominio Active Directory e sostituiscilo `389` con la porta LDAP per il tuo ambiente.
   > Verifica di aver aperto le porte richieste all'interno del firewall.

Di seguito è riportato un esempio di test nping riuscito in cui il gateway è riuscito a raggiungere il controller di dominio:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>
```

```
Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

Di seguito è riportato un esempio di test nping in cui non c'è connettività o risposta dalla `corp.domain.com` destinazione:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Verifica le opzioni DHCP impostate per il VPC della tua istanza Amazon gateway EC2

Se File Gateway è in esecuzione su un' EC2 istanza Amazon, devi assicurarti che un set di opzioni DHCP sia configurato e collegato correttamente all'Amazon Virtual Private Cloud (VPC) che contiene l'istanza del gateway. Per ulteriori informazioni, consulta Set di opzioni DHCP in Amazon VPC.

Verifica che il gateway sia in grado di risolvere il dominio eseguendo una query dig

Se il dominio non è risolvibile dal gateway, il gateway non può entrare a far parte del dominio.

Per eseguire una dig query:

1. Connect alla console locale del gateway utilizzando il software di gestione dell'hypervisor (VMwareHyper-V o KVM) per i gateway locali o utilizzando ssh per i gateway Amazon. EC2
2. Inserisci il numero corrispondente per selezionare Gateway Console, quindi inserisci per elencare tutti i comandi disponibili. h Per verificare se il gateway è in grado di risolvere il dominio, esegui il comando seguente:

   ```
   dig -d corp.domain.com
   ```

> **Note**
>
> `corp.domain.com`Sostituiscilo con il nome DNS del dominio Active Directory.

Di seguito è riportato un esempio di risposta riuscita:

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

Controlla le impostazioni e i ruoli del controller di dominio

Verifica che il controller di dominio non sia impostato in modalità di sola lettura e che disponga di ruoli sufficienti per consentire l'accesso ai computer. Per verificarlo, prova a collegare altri server dalla stessa sottorete VPC della macchina virtuale gateway al dominio.

Verifica che il gateway sia aggiunto al controller di dominio più vicino

Come procedura ottimale, si consiglia di collegare il gateway a un controller di dominio geograficamente vicino all'appliance gateway. Se l'appliance gateway non è in grado di comunicare con il controller di dominio entro 20 secondi a causa della latenza di rete, il processo di aggiunta al dominio può scadere. Ad esempio, il processo potrebbe scadere se l'appliance gateway si trova negli

Stati Uniti orientali (Virginia settentrionale) Regione AWS e il controller di dominio si trova nell'Asia Pacifico (Singapore). Regione AWS

> **Note**
>
> Per aumentare il valore di timeout predefinito di 20 secondi, è possibile eseguire il comando join-domain in AWS Command Line Interface (AWS CLI) e includere l'`--timeout-in-seconds`opzione per aumentare il tempo. Puoi anche utilizzare la chiamata JoinDomain API e includere il `TimeoutInSeconds` parametro per aumentare il tempo. Il valore di timeout massimo è di 3.600 secondi.
> Se ricevi errori durante l'esecuzione dei AWS CLI comandi, assicurati di utilizzare la versione più recente. AWS CLI

Verifica che Active Directory crei nuovi oggetti informatici nell'unità organizzativa (OU) predefinita

Accertarsi che Microsoft Active Directory non disponga di oggetti di criteri di gruppo che creino nuovi oggetti computer in posizioni diverse dall'unità organizzativa predefinita. Prima di poter aggiungere il gateway al dominio Active Directory, è necessario che nell'unità organizzativa predefinita esista un nuovo oggetto computer. Alcuni ambienti Active Directory sono personalizzati in modo da avere oggetti diversi OUs per quelli appena creati. Per garantire che nell'unità organizzativa predefinita esista un nuovo oggetto computer per la macchina virtuale gateway, provate a creare l'oggetto computer manualmente sul controller di dominio prima di aggiungere il gateway al dominio. È inoltre possibile eseguire il comando join-domain utilizzando. AWS CLI Quindi, specifica l'opzione per. `--organizational-unit`

> **Note**
>
> Il processo di creazione dell'oggetto informatico è denominato preallestimento.

Controlla i registri degli eventi del controller di dominio

Se non riesci ad aggiungere il gateway al dominio dopo aver provato tutti gli altri controlli e configurazioni descritti nelle sezioni precedenti, ti consigliamo di esaminare i registri degli eventi del controller di dominio. Verifica la presenza di eventuali errori nel visualizzatore eventi del controller di dominio. Verifica che le query del gateway abbiano raggiunto il controller di dominio.

Risoluzione dei problemi: errore interno durante l'attivazione del gateway

Le richieste di attivazione dello Storage Gateway attraversano due percorsi di rete. Le richieste di attivazione in entrata inviate da un client si connettono alla macchina virtuale (VM) o all'istanza Amazon Elastic Compute Cloud (Amazon EC2) del gateway tramite la porta 80. Se il gateway riceve correttamente la richiesta di attivazione, comunica con gli endpoint Storage Gateway per ricevere una chiave di attivazione. Se il gateway non riesce a raggiungere gli endpoint Storage Gateway, risponde al client con un messaggio di errore interno.

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se ricevi un messaggio di errore interno quando tenti di attivare il. Gateway di archiviazione AWS

> **Note**
>
> - Assicurati di distribuire nuovi gateway utilizzando l'ultimo file di immagine della macchina virtuale o la versione di Amazon Machine Image (AMI). Riceverai un errore interno se tenti di attivare un gateway che utilizza un'AMI obsoleta.
> - Assicurati di selezionare il tipo di gateway corretto che intendi implementare prima di scaricare l'AMI. I file.ova e AMIs per ogni tipo di gateway sono diversi e non sono intercambiabili.

Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico

Per risolvere gli errori di attivazione durante l'attivazione del gateway utilizzando un endpoint pubblico, esegui i seguenti controlli e configurazioni.

Controlla le porte richieste

Per i gateway distribuiti in locale, verifica che le porte sul firewall locale siano aperte. Per i gateway distribuiti su un' EC2 istanza Amazon, verifica che le porte siano aperte nel gruppo di sicurezza dell'istanza. Per confermare che le porte siano aperte, esegui un comando telnet sull'endpoint pubblico da un server. Questo server deve trovarsi nella stessa sottorete del gateway. Ad esempio, i seguenti comandi telnet testano la connessione alla porta 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Per confermare che il gateway stesso possa raggiungere l'endpoint, accedi alla console VM locale del gateway (per i gateway distribuiti in locale). In alternativa, puoi accedere tramite SSH all'istanza del gateway (per i gateway distribuiti su Amazon). EC2 Quindi, esegui un test di connettività di rete. Conferma che il test ritorni`[PASSED]`. Per ulteriori informazioni, vedi Test della connettività di rete del gateway .

> **Note**
>
> Il nome utente di accesso predefinito per la console del gateway è`admin`, e la password predefinita è`password`.

Assicurati che la sicurezza del firewall non modifichi i pacchetti inviati dal gateway agli endpoint pubblici

Le ispezioni SSL, le ispezioni approfondite dei pacchetti o altre forme di sicurezza del firewall possono interferire con i pacchetti inviati dal gateway. L'handshake SSL fallisce se il certificato SSL viene modificato rispetto a quanto previsto dall'endpoint di attivazione. Per confermare che non è in corso alcuna ispezione SSL, esegui un comando OpenSSL sull'endpoint `anon-cp.storagegateway.region.amazonaws.com` di attivazione principale () sulla porta 443. È necessario eseguire questo comando da un computer che si trova nella stessa sottorete del gateway:

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Sostituisci *`region`* con il tuo. Regione AWS

Se non è in corso alcuna ispezione SSL, il comando restituisce una risposta simile alla seguente:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Se è in corso un'ispezione SSL, la risposta mostra una catena di certificati alterata, simile alla seguente:

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

L'endpoint di attivazione accetta gli handshake SSL solo se riconosce il certificato SSL. Ciò significa che il traffico in uscita del gateway verso gli endpoint deve essere esente dalle ispezioni eseguite dai firewall della rete. Queste ispezioni possono essere un'ispezione SSL o un'ispezione approfondita dei pacchetti.

Controlla la sincronizzazione dell'ora del gateway

Scostamenti temporali eccessivi possono causare errori di handshake SSL. Per i gateway locali, è possibile utilizzare la console VM locale del gateway per controllare la sincronizzazione dell'ora del gateway. L'inclinazione temporale non deve superare i 60 secondi.

L'opzione System Time Management non è disponibile sui gateway ospitati su EC2 istanze Amazon. Per assicurarti che i EC2 gateway Amazon possano sincronizzare correttamente l'ora, verifica che l' EC2 istanza Amazon possa connettersi al seguente elenco di pool di server NTP tramite le porte UDP e TCP 123:

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint Amazon VPC

Per risolvere gli errori di attivazione durante l'attivazione del gateway utilizzando un endpoint Amazon Virtual Private Cloud (Amazon VPC), esegui i seguenti controlli e configurazioni.

Controlla le porte richieste

Assicurati che le porte richieste all'interno del firewall locale (per i gateway distribuiti in locale) o del gruppo di sicurezza (per i gateway distribuiti in Amazon) siano aperte. EC2 Le porte necessarie per connettere un gateway a un endpoint VPC Storage Gateway sono diverse da quelle richieste per la connessione di un gateway a endpoint pubblici. Le seguenti porte sono necessarie per la connessione a un endpoint VPC Storage Gateway:

- TCP 443

- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Inoltre, controlla il gruppo di sicurezza collegato all'endpoint VPC dello Storage Gateway. Il gruppo di sicurezza predefinito collegato all'endpoint potrebbe non consentire le porte richieste. Crea un nuovo gruppo di sicurezza che consenta il traffico proveniente dall'intervallo di indirizzi IP del gateway sulle porte richieste. Quindi, collega quel gruppo di sicurezza all'endpoint VPC.

> **Note**
>
> Utilizza la console Amazon VPC per verificare il gruppo di sicurezza collegato all'endpoint VPC. Visualizza l'endpoint VPC Storage Gateway dalla console, quindi scegli la scheda Security Groups.

Per confermare che le porte richieste siano aperte, è possibile eseguire i comandi telnet sull'endpoint VPC Storage Gateway. È necessario eseguire questi comandi da un server che si trova nella stessa sottorete del gateway. È possibile eseguire i test sul primo nome DNS che non specifica una zona di disponibilità. Ad esempio, i seguenti comandi telnet testano le connessioni alle porte richieste utilizzando il nome DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Assicurati che la sicurezza del firewall non modifichi i pacchetti inviati dal gateway all'endpoint Amazon VPC di Storage Gateway

Le ispezioni SSL, le ispezioni approfondite dei pacchetti o altre forme di sicurezza del firewall possono interferire con i pacchetti inviati dal gateway. L'handshake SSL fallisce se il certificato SSL

viene modificato rispetto a quanto previsto dall'endpoint di attivazione. Per confermare che non è in corso alcuna ispezione SSL, esegui un comando OpenSSL sull'endpoint VPC Storage Gateway. È necessario eseguire questo comando da un computer che si trova nella stessa sottorete del gateway. Esegui il comando per ogni porta richiesta:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Se non è in corso alcuna ispezione SSL, il comando restituisce una risposta simile alla seguente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
```

```
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Se è in corso un'ispezione SSL, la risposta mostra una catena di certificati alterata, simile alla seguente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

L'endpoint di attivazione accetta gli handshake SSL solo se riconosce il certificato SSL. Ciò significa che il traffico in uscita del gateway verso l'endpoint VPC sulle porte richieste è esente dalle ispezioni eseguite dai firewall di rete. Queste ispezioni potrebbero essere ispezioni SSL o ispezioni approfondite dei pacchetti.

Controlla la sincronizzazione dell'ora del gateway

Scostamenti temporali eccessivi possono causare errori di handshake SSL. Per i gateway locali, è possibile utilizzare la console VM locale del gateway per controllare la sincronizzazione dell'ora del gateway. L'inclinazione temporale non deve superare i 60 secondi.

L'opzione System Time Management non è disponibile sui gateway ospitati su EC2 istanze Amazon. Per assicurarti che i EC2 gateway Amazon possano sincronizzare correttamente l'ora, verifica che l' EC2 istanza Amazon possa connettersi al seguente elenco di pool di server NTP tramite le porte UDP e TCP 123:

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Verifica la presenza di un proxy HTTP e conferma le impostazioni del gruppo di sicurezza associato

Prima dell'attivazione, verifica se hai un proxy HTTP su Amazon EC2 configurato sulla macchina virtuale gateway locale come proxy Squid sulla porta 3128. In questo caso, conferma quanto segue:

- Il gruppo di sicurezza collegato al proxy HTTP su Amazon EC2 deve avere una regola in entrata. Questa regola in entrata deve consentire il traffico proxy Squid sulla porta 3128 dall'indirizzo IP della macchina virtuale del gateway.
- Il gruppo di sicurezza collegato all'endpoint Amazon EC2 VPC deve avere regole in entrata. Queste regole in entrata devono consentire il traffico sulle porte 1026-1028, 1031, 2222 e 443 dall'indirizzo IP del proxy HTTP su Amazon. EC2

Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico e nello stesso VPC è presente un endpoint VPC Storage Gateway

Per risolvere gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico quando è presente un enpoint Amazon Virtual Private Cloud (Amazon VPC) nello stesso VPC, esegui i seguenti controlli e configurazioni.

Verificare che l'impostazione Enable Private DNS Name non sia abilitata sull'endpoint VPC Storage Gateway

Se l'opzione Abilita nome DNS privato è abilitata, non è possibile attivare alcun gateway da quel VPC all'endpoint pubblico.

Per disabilitare l'opzione del nome DNS privato:

1. Apri la Console Amazon VPC.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Scegli il tuo endpoint VPC Storage Gateway.
4. Scegli Azioni.
5. Scegli Gestisci nomi DNS privati.
6. Per Abilita nome DNS privato, deseleziona Abilita per questo endpoint.
7. Scegli Modifica nomi DNS privati per salvare l'impostazione.

Risoluzione dei problemi: problemi relativi al gateway locale

Di seguito sono riportate informazioni sui problemi tipici che potresti riscontrare lavorando con i gateway locali e su come consentire la connessione Supporto al gateway per facilitare la risoluzione dei problemi.

Nella tabella seguente sono elencati i più comuni problemi che potrebbero verificarsi utilizzando gateway distribuiti in locale.

Problema	Operazione da eseguire
Non è possibile reperire l'indirizzo IP del gateway.	Utilizzare il client dell'hypervisor per connettersi all'host e trovare l'indirizzo IP del gateway. • Infatti VMware ESXi, l'indirizzo IP della macchina virtuale è disponibile nel client vSphere nella scheda Riepilogo. • Per Microsoft Hyper-V, l'indirizzo IP della VM può essere reperito accedendo alla console locale. Se comunque non si trova l'indirizzo IP del gateway:

Problema	Operazione da eseguire
	• Controllare che la VM sia attiva. Solo una VM attiva, infatti, consente l'assegnazione di un indirizzo IP al gateway. • Attendere la conclusione della procedura di avvio della VM. Con la VM appena attivata, la sequenza di avvio del gateway potrebbe richiedere qualche minuto per terminare.
Si verificano problemi di firewall o rete.	• Abilitare le porte necessarie per il gateway. • Se si utilizza un firewall o un router per filtrare o limitare il traffico di rete, è necessario configurare il firewall e/o il router affinché consentano questi endpoint di servizio per le comunicazioni in uscita ad AWS. Per ulteriori informazioni sui requisiti di rete e del firewall, consulta Requisiti di rete e firewall.
L'attivazione del gateway non riesce se si fa clic sul pulsante Continua con l'attivazione nella console di gestione Storage Gateway.	• Verificare l'accessibilità della VM del gateway eseguendone il ping dal client. • Verificare la connettività di rete a Internet della VM, senza la quale occorrerà configurare un proxy SOCKS. Per ulteriori informazioni in merito, consulta Verifica della connettività di rete del gateway. • Verificare che gli orari dell'host e della VM del gateway siano corretti e che l'host sia configurato per la sincronizzazione automatica di data e ora con un server NTP (Network Time Protocol). Per informazioni sulla sincronizzazione dell'ora degli host dell'hypervisor e, vedere. VMs Configurazione di un server Network Time Protocol (NTP) per il gateway • Dopo queste fasi, è possibile riprovare l'implementazione del gateway con la console Storage Gateway e la procedura guidata Configura e attiva il gateway. • Verifica che la tua macchina virtuale abbia almeno 16 GB di RAM. L'allocazione del gateway fallisce se la RAM è inferiore a 16 GB. Per ulteriori informazioni, consulta Requisiti di configurazione di File Gate.

Problema	Operazione da eseguire
Occorre aumentare la larghezza di banda tra il gateway e AWS.	È possibile migliorare la larghezza di banda dal gateway al AWS configurando la connessione Internet AWS su un adattatore di rete (NIC) separato da quello che collega le applicazioni e la macchina virtuale del gateway. Questo approccio è utile se si dispone di una connessione a larghezza di banda elevata AWS e si desidera evitare conflitti in termini di larghezza di banda, specialmente durante il ripristino di un'istantanea. Utilizzando Direct Connect si può stabilire una connessione di rete dedicata tra il gateway on-premise e AWS, perfetta per i carichi di lavoro con elevata velocità di trasmissione effettiva. Per misurare la larghezza di banda della connessione dal gateway a AWS, utilizza le metriche e del `CloudBytesDownloaded` gateway. `CloudBytesUploaded` Per ulteriori informazioni su questo argomento, consulta Prestazioni e ottimizzazione. Ottimizzando la connettività a Internet si evita il riempimento del buffer di caricamento.

Problema	Operazione da eseguire

Il throughput da o verso il gateway si azzera.	• Nella scheda Gateway della console Storage Gateway, verifica che gli indirizzi IP per la macchina virtuale gateway siano gli stessi visualizzati utilizzando il software client hypervisor (ovvero il client VMware vSphere o Microsoft Hyper-V Manager). In caso di mancata corrispondenza, riavviare il gateway dalla console Storage Gateway, come illustrato in Spegnimento della macchina virtuale gateway. Dopo il riavvio, gli indirizzi dell'elenco Indirizzi IP nella scheda Gateway della console Storage Gateway dovrebber o corrispondere agli indirizzi IP del gateway, determinati dal client dell'hypervisor.
	  • Infatti VMware ESXi, l'indirizzo IP della macchina virtuale è disponibile nel client vSphere nella scheda Riepilogo.
	  • Per Microsoft Hyper-V, l'indirizzo IP della VM può essere reperito accedendo alla console locale.
	• Verifica la connettività del gateway a AWS come descritto in. Verifica della connettività di rete del gateway
	• Controlla la configurazione dell'adattatore di rete del gateway nel client di gestione dell'hypervisor e assicurati che tutte le interfacc e che intendi utilizzare per il gateway siano attivate.
	• Controlla la configurazione dell'adattatore di rete del gateway nella console locale del gateway. Per istruzioni, consulta Configurazione delle impostazioni di rete del gateway.
	
	Puoi visualizzare la velocità effettiva da e verso il gateway dalla CloudWatch console Amazon. Per ulteriori informazioni sulla misurazione della velocità effettiva da e verso il gateway di destinazi one AWS, consulta. Prestazioni e ottimizzazione

Si sono verificati problemi durante l'importazione (distribuzione) di Storage Gateway su Microsoft Hyper-V.	Consultare Risoluzione dei problemi: configurazione di Microsoft Hyper-V, documento dedicato ai problemi che più comunemente possono verificarsi distribuendo un gateway su Microsoft Hyper-V.

Problema	Operazione da eseguire
Viene visualizzato il seguente messaggio: "I dati scritti sul volume del gateway non sono archiviati in modo sicuro su AWS".	Questo messaggio viene ricevuto se la VM del gateway è stata creata da un clone o uno snapshot di un'altra VM di gateway. Se così non fosse, rivolgersi a Supporto.

Risoluzione dei problemi: le scansioni di sicurezza mostrano porte NFS aperte

Alcune porte NFS sono abilitate per impostazione predefinita, anche sui gateway utilizzati solo con le condivisioni di file SMB. Se si utilizza un software di sicurezza di terze parti come Qualys per scansionare la rete in cui è distribuito File Gateway, i risultati della scansione potrebbero segnalare queste porte NFS aperte come una potenziale vulnerabilità di sicurezza. Se utilizzate il gateway solo con condivisioni di file SMB e desiderate disabilitare le porte NFS non utilizzate per motivi di sicurezza, utilizzate la seguente procedura:

Per disabilitare le porte NFS su un File Gateway:

1. Accedere al prompt dei comandi della console locale del gateway utilizzando la procedura descritta in. Esecuzione di comandi Storage Gateway sulla console locale
2. Immettete i seguenti comandi per disabilitare il traffico NFS:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ```

```
ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. Immettete il seguente comando per confermare che le porte NFS bloccate vengano visualizzate nelle tabelle IP:

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

Attivazione dell' Supporto accesso per facilitare la risoluzione dei problemi relativi al gateway ospitato in locale

Storage Gateway fornisce una console locale che può essere utilizzata per eseguire diverse attività di manutenzione, tra cui consentire l'accesso Supporto al gateway per facilitare la risoluzione dei problemi relativi al gateway. Per impostazione predefinita, Supporto l'accesso al gateway è disattivato. È possibile attivare questo accesso tramite la console locale dell'host. Per Supporto consentire l'accesso al gateway, è necessario innanzitutto accedere alla console locale dell'host, accedere alla console di Storage Gateway e quindi connettersi al server di supporto.

Per attivare Supporto l'accesso al gateway

1. Accedere alla console locale dell'host.

   - VMware ESXi — per ulteriori informazioni, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Microsoft Hyper-V: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Microsoft Hyper-V.

2. Quando richiesto, immetti il numero corrispondente per selezionare Console gateway.
3. Immetti **h** per aprire la finestra dei comandi disponibili.
4. Esegui una delle seguenti operazioni:

- Se il gateway utilizza un endpoint pubblico, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`** per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.
- Se il gateway utilizza un endpoint VPC, nella finestra COMANDI DISPONIBILI, inserisci **`open-support-channel`**. Se il gateway non è attivato, fornire l'endpoint VPC o l'indirizzo IP per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

> **Note**
>
> Il numero del canale non è un numero di porta Protocol/User Datagram Protocol (TCP/UDP (Transmission Control). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server di Storage Gateway e su questa mette a disposizione il canale di supporto.

5. Dopo aver stabilito il canale di supporto, fornisci il numero del servizio di supporto Supporto in modo da Supporto poter fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **`q`** per terminare. Non chiudere la sessione finché il supporto di Amazon Web Services non comunica che la sessione di supporto è completa.
7. Immettere **`exit`** per disconnettersi dalla console Storage Gateway.
8. Seguire le istruzioni per uscire dalla console locale.

Risoluzione dei problemi: configurazione di Microsoft Hyper-V

Nella tabella seguente sono elencati i problemi che più comunemente possono verificarsi quando si implementa Storage Gateway sulla piattaforma Microsoft Hyper-V.

Problema	Operazione da eseguire
Si tenta di importare un gateway e si riceve il	Ci si può imbattere in questo errore per i seguenti motivi:

Problema	Operazione da eseguire
seguente messaggio di errore: «Si è verificato un errore del server durante il tentativo di importare la macchina virtuale. Importazione non riuscita. Impossibile trovare i file di importazione della macchina virtuale nella posizione [...]. Puoi importare una macchina virtuale solo se hai usato Hyper-V per crearla ed esportarla.»	• Se non si specifica l'origine dei file sorgente decompressi del gateway. L'ultima parte della posizione specificata nella finestra di dialogo Importa macchina virtuale dovrebbe essere. `AWS-Storage-Gateway` Esempio: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\ .` • Se è già stato distribuito un gateway senza selezionare le opzioni Copy the virtual machine (Copia la macchina virtuale) e Duplicate all files (Duplica tutti i file) nella finestra di dialogo Import Virtual Machine (Importa macchina virtuale), la VM è stata già creata nella sede dove si trovano i file di gateway decompressi, dalla quale non è possibile importare nuovamente. Per risolvere il problema, copiare ex novo i file sorgente del gateway decompressi in una nuova sede, da utilizzare come origine d'importazione. Se si prevede di creare più gateway da un'unica posizione di file di origine decompressi, è necessario selezionare Copia la macchina virtuale e selezionare la casella Duplica tutti i file nella finestra di dialogo Importa macchina virtuale.
Si tenta di importare un gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore del server durante il tentativo di importare la macchina virtuale. Importazione non riuscita. L'operazione di importazione non è riuscita a copiare il file da [...]: il file esiste. (0x80070050)»	Questo errore si verifica quando, con un gateway già distribuito, si tenta di riutilizzare le cartelle predefinite che includono i file del disco rigido virtuale e quelli di configurazione della macchina virtuale. Per risolvere questo problema, specifica nuove posizioni in Server nel pannello sul lato sinistro della finestra di dialogo Impostazioni Hyper-V.

Problema	Operazione da eseguire
Si tenta di importare un gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore del server durante il tentativo di importare la macchina virtuale. Importazione non riuscita. Per importare, assegna alla macchina virtuale un nuovo identificatore. Seleziona il nuovo identificatore e riprova."	Quando importi il gateway, assicurati di selezionare Copia la macchina virtuale e di selezionare la casella Duplica tutti i file nella finestra di dialogo Importa macchina virtuale per creare un nuovo ID univoco per la macchina virtuale.
Si tenta di avviare una macchina virtuale gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore durante il tentativo di avviare le macchine virtuali selezionate. L'imposta zione del processore di partizione secondario non è compatibile con la partizione principale. Impossibile inizializzare 'AWS-Storage-Gateway'. (ID macchina virtuale [...])»	Questo errore è probabilmente causato da una discrepanza della CPU tra quella richiesta CPUs per il gateway e quella disponibi le CPUs sull'host. Accertarsi che il conteggio di CPU della VM sia supportato dall'hypervisor sottostante. Per ulteriori informazioni sui requisiti per Storage Gateway, consulta Requisiti di configurazione di File Gate.

Problema	Operazione da eseguire
Si tenta di avviare una macchina virtuale gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore durante il tentativo di avviare le macchine virtuali selezionate. Impossibile inizializzare 'AWS-Storage-Gateway'. (ID macchina virtuale [...]) Impossibile creare la partizione: le risorse di sistema sono insufficienti per completar e il servizio richiesto. (0x800705AA)»	Questo errore potrebbe essere causato da una discrepanza tra la RAM necessaria per il gateway e quella disponibile sull'host. Per ulteriori informazioni sui requisiti per Storage Gateway, consulta Requisiti di configurazione di File Gate.
Gli aggiornamenti di software di gateway e snapshot si verificano con tempistiche leggermente diverse da quelle previste.	L'orologio della VM del gateway potrebbe essere soggetto allo scostamento del clock, cioè differire dall'orario effettivo. Controlla re e correggere l'orario della VM utilizzando l'opzione di sincroniz zazione oraria della console del gateway locale. Per ulteriori informazioni, consulta Configurazione di un server Network Time Protocol (NTP) per il gateway.
Bisogna inserire i file decompressi di Storage Gateway con Microsoft Hyper-V nel file system dell'host.	Accedere all'host come si fa generalmente con un server Microsoft Windows. Ad esempio, se il nome dell'host dell'hypervisor è `hyperv-server` , si può utilizzare il percorso UNC `\\hyperv-server\c$` , presupponendo che il nome `hyperv-server` possa essere risolto o sia definito nel file degli host in locale.
Nel connettersi all'hyper visor viene richiesto di immettere le credenziali.	Aggiungere le credenziali utente da amministratore locale per l'host dell'hypervisor, avvalendosi dello strumento Sconfig.cmd.

Problema	Operazione da eseguire
È possibile notare prestazioni di rete scadenti se si attiva la coda di macchine virtuali (VMQ) per un host Hyper-V che utilizza una scheda di rete Broadcom.	Per informazioni su una soluzione alternativa, consulta la documentazione Microsoft, vedi Scarse prestazioni di rete sulle macchine virtuali su un host Hyper-V Windows Server 2012 se VMQ è acceso.

Risoluzione dei problemi: problemi relativi al EC2 gateway Amazon

Nelle sezioni seguenti, puoi trovare i problemi tipici che potresti riscontrare lavorando con il tuo gateway distribuito su Amazon EC2. Per ulteriori informazioni sulla differenza tra un gateway locale e un gateway distribuito in Amazon EC2, consulta. Implementa un EC2 host Amazon predefinito per S3 File Gateway

Per informazioni sull'utilizzo dello storage temporaneo, consulta Utilizzo dello storage temporaneo con i gateway EC2 .

Argomenti

- Dopo qualche secondo, il gateway ancora non si attiva
- Non riesci a trovare l'istanza del EC2 gateway nell'elenco delle istanze
- Vuoi connetterti alla tua istanza gateway utilizzando la console EC2 seriale Amazon
- Vuoi aiutarci Supporto a risolvere i problemi del tuo gateway Amazon EC2

Dopo qualche secondo, il gateway ancora non si attiva

Controlla quanto segue nella EC2 console Amazon:

- La porta 80 è aperta nel gruppo di sicurezza associato all'istanza. Per ulteriori informazioni sull'aggiunta di una regola del gruppo di sicurezza, consulta Adding a security group rule nella Amazon EC2 User Guide.
- L'istanza del gateway è contrassegnata come in esecuzione. Nella EC2 console Amazon, il valore State per l'istanza deve essere RUNNING.

- Assicurati che il tuo tipo di EC2 istanza Amazon soddisfi i requisiti minimi, come descritto inRequisiti di storage.

Dopo aver risolto il problema, provare di nuovo ad attivare il gateway. A tale scopo, apri la console Storage Gateway, scegli Implementa un nuovo gateway su Amazon EC2 e inserisci nuovamente l'indirizzo IP dell'istanza.

Non riesci a trovare l'istanza del EC2 gateway nell'elenco delle istanze

Se non si assegna all'istanza un tag di risorsa e si dispone di molte istanze in esecuzione, può risultare difficile stabilire quale istanza è stata avviata. Per individuare l'istanza del gateway, in tal caso, occorre procedere come di seguito:

- Controllare il nome dell'Amazon Machine Image (AMI) nella scheda Description (Descrizione) dell'istanza. Il nome di un'istanza basata sull'AMI di Storage Gateway dovrebbe iniziare con il testo **`aws-storage-gateway-ami`**.
- Se si dispone di più istanze basate sull'AMI di Storage Gateway, controllarne l'orario di avvio per trovare quella giusta.

Vuoi connetterti alla tua istanza gateway utilizzando la console EC2 seriale Amazon

Puoi utilizzare la console EC2 seriale di Amazon per risolvere problemi di avvio, configurazione di rete e altri problemi. Per istruzioni e suggerimenti per la risoluzione dei problemi, consulta Amazon EC2 Serial Console nella Amazon Elastic Compute Cloud User Guide.

Vuoi aiutarci Supporto a risolvere i problemi del tuo gateway Amazon EC2

Storage Gateway fornisce una console locale che può essere utilizzata per eseguire diverse attività di manutenzione, tra cui consentire l'accesso Supporto al gateway per facilitare la risoluzione dei problemi relativi al gateway. Per impostazione predefinita, Supporto l'accesso al gateway è disattivato. Attivi questo accesso tramite la console EC2 locale di Amazon. Accedi alla console EC2 locale di Amazon tramite Secure Shell (SSH). Per effettuare l'accesso tramite SSH, il gruppo di sicurezza dell'istanza deve contenere una regola che apra la porta TCP 22.

> **Note**
>
> Se si aggiunge una nuova regola a un gruppo di sicurezza, la nuova regola si applica a tutte le istanze che utilizzano quel gruppo di sicurezza. Per ulteriori informazioni sui gruppi di sicurezza e su come aggiungere una regola per i gruppi di sicurezza, consulta i gruppi EC2 di sicurezza Amazon nella Amazon EC2 User Guide.

Per consentire la Supporto connessione al gateway, devi prima accedere alla console locale dell' EC2 istanza Amazon, accedere alla console di Storage Gateway e quindi fornire l'accesso.

Per attivare Supporto l'accesso per un gateway distribuito su un'istanza Amazon EC2

1. Accedi alla console locale per la tua EC2 istanza Amazon. Per istruzioni, consulta Connect to your istance nella Amazon EC2 User Guide.

   Puoi usare il seguente comando per accedere alla console locale dell' EC2 istanza.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*È il `.pem` file contenente il certificato privato della coppia di EC2 chiavi che hai usato per avviare l' EC2 istanza Amazon. Per ulteriori informazioni, consulta Recupero della chiave pubblica per la tua coppia di chiavi nella Amazon EC2 User Guide.
   > *INSTANCE-PUBLIC-DNS-NAME*è il nome DNS (Domain Name System) pubblico dell' EC2 istanza Amazon su cui è in esecuzione il gateway. Puoi ottenere questo nome DNS pubblico selezionando l' EC2istanza Amazon nella EC2 console e facendo clic sulla scheda Descrizione.

2. Quando richiesto, immettere **`6 - Command Prompt`** per aprire la console del canale Supporto .
3. Immettere **`h`** per aprire la finestra AVAILABLE COMMANDS (COMANDI DISPONIBILI).
4. Esegui una delle seguenti operazioni:

   - Se il gateway utilizza un endpoint pubblico, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`** per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci

si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

- Se il gateway utilizza un endpoint VPC, nella finestra COMANDI DISPONIBILI, inserisci **`open-support-channel`**. Se il gateway non è attivato, fornire l'endpoint VPC o l'indirizzo IP per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

> **Note**
>
> Il numero del canale non è un numero di porta Protocol/User Datagram Protocol (TCP/UDP (Transmission Control). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server di Storage Gateway e su questa mette a disposizione il canale di supporto.

5. Dopo aver stabilito il canale di supporto, fornisci il numero del servizio di supporto Supporto in modo da Supporto poter fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **`q`** per terminare. Non chiudere la sessione finché il supporto di Amazon Web Services non comunica che la sessione di supporto è completa.
7. Inserisci **`exit`** per uscire dalla console Storage Gateway.
8. Segui i menu della console per uscire dall'istanza Storage Gateway.

Risoluzione dei problemi: problemi relativi alle apparecchiature hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Negli argomenti seguenti vengono descritti i problemi che potrebbero verificarsi con l'appliance hardware AWS Storage Gateway e suggerimenti per risolverli.

Argomenti

- Impossibile determinare l'indirizzo IP del servizio
- Come si esegue una reimpostazione ai valori di fabbrica?
- Come si esegue il riavvio remoto?
- Dove si ottiene il supporto Dell iDRAC?
- Impossibile trovare il numero di serie dell'appliance hardware
- Dove ottenere supporto per l'appliance hardware

Impossibile determinare l'indirizzo IP del servizio

Durante il tentativo di connessione al servizio, assicurarsi di utilizzare l'indirizzo IP del servizio e non l'indirizzo IP dell'host. Configurare l'indirizzo IP del servizio nella console di servizio e l'indirizzo IP dell'host nella console hardware. La console hardware viene visualizzata quando si avvia l'appliance hardware. Per accedere alla console di servizio dalla console hardware, scegliere Open Service Console (Apri console di servizio).

Come si esegue una reimpostazione ai valori di fabbrica?

Se è necessario eseguire un ripristino delle impostazioni di fabbrica sul dispositivo, contattare il team di AWS Storage Gateway Hardware Appliance per ricevere assistenza, come descritto nella sezione Supporto che segue.

Come si esegue il riavvio remoto?

Se è necessario eseguire un riavvio remoto del dispositivo, è possibile farlo utilizzando l'interfaccia di gestione Dell iDRAC. Per ulteriori informazioni, consulta DRAC9 Virtual Power Cycle: accensione remota dei PowerEdge server Dell EMC sul sito Web di Dell Technologies. InfoHub

Dove si ottiene il supporto Dell iDRAC?

Il PowerEdge server Dell è dotato dell'interfaccia di gestione Dell iDRAC. Consigliamo quanto segue:

- Se si utilizza l'interfaccia di gestione iDRAC, è necessario modificare la password predefinita. Per ulteriori informazioni sulle credenziali iDRAC, vedere PowerEdge Dell - Quali sono le credenziali di accesso predefinite per iDRAC? .

- Assicurati che il firmware up-to-date serva a prevenire violazioni della sicurezza.
- Spostare l'interfaccia di rete iDRAC su una porta normale (`em`) può causare problemi di prestazioni o prevenire il normale funzionamento dell'appliance.

Impossibile trovare il numero di serie dell'appliance hardware

È possibile trovare il numero di serie dell'appliance hardware AWS Storage Gateway utilizzando la console Storage Gateway.

Per trovare il numero di serie del dispositivo hardware:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Dal menu di navigazione a sinistra della pagina, scegli Hardware.
3. Seleziona il tuo dispositivo hardware dall'elenco.
4. Individua il campo Numero di serie nella scheda Dettagli del tuo dispositivo.

Dove ottenere supporto per l'appliance hardware

Per contattare il supporto tecnico AWS relativo al dispositivo hardware, vedere. Supporto

Il Supporto team potrebbe chiederti di attivare il canale di supporto per risolvere i problemi relativi al gateway da remoto. Non è necessario che questa porta sia aperta per il normale funzionamento del gateway, ma è necessario per la risoluzione dei problemi. È possibile attivare il canale di supporto dalla console hardware, come illustrato nella procedura seguente.

Per aprire un canale di supporto per AWS

1. Aprire la console hardware.
2. Scegli Open Support Channel nella parte inferiore della pagina principale della console hardware, quindi premi`Enter`.

   Il numero di porta assegnato dovrebbe apparire entro 30 secondi se non ci sono problemi di connettività di rete o firewall. Esempio:

   Stato: Aperto sulla porta 19599
3. Annota il numero di porta e forniscilo a Supporto.

Risoluzione dei problemi: problemi relativi a File Gateway

Puoi configurare File Gateway per scrivere voci di registro in un gruppo di CloudWatch log Amazon. In tal caso, riceverai notifiche sullo stato di integrità del gateway e su eventuali errori riscontrati dal gateway. È possibile trovare informazioni su queste notifiche di errore e di integrità in CloudWatch Logs.

Nelle sezioni seguenti sono disponibili informazioni che consentono di comprendere la causa di ogni errore e notifica di integrità e come risolvere i problemi.

Argomenti

- Errore: 1344 (0x00000540)
- Errore: GatewayClockOutOfSync
- Errore: InaccessibleStorageClass
- Errore: InvalidObjectState
- Errore: ObjectMissing
- Errore: RoleTrustRelationshipInvalid
- Errore: S3 AccessDenied
- Errore: DroppedNotifications
- Notifica: HardReboot
- Notifica: riavvio
- Risoluzione dei problemi: le scansioni di sicurezza mostrano porte NFS aperte
- Risoluzione dei problemi: utilizzo CloudWatch delle metriche

Errore: 1344 (0x00000540)

Durante la migrazione di file su Amazon S3, potresti riscontrare `ERROR 1344 (0x00000540)` un errore se stai tentando di copiare file con più di 10 Access Control Entries ACEs () in Amazon S3. Le voci di controllo degli accessi sono elencate nell'Access Control List (ACL).

Amazon S3 File Gateway può conservare solo 10 voci ACE per file o cartella.

Per risolvere un errore 1344: copia di NTFS Security nella directory di destinazione.

Ridurre il numero di voci nelle autorizzazioni di Windows per file o cartelle che contengono più di 10 voci. Un approccio comune consiste nel creare un gruppo contenente l'elenco completo delle voci,

quindi sostituire l'elenco di voci con quel singolo gruppo. Una volta che il numero di voci è inferiore a 10, è possibile riprovare a copiare i file o le cartelle sul gateway.

Errore: GatewayClockOutOfSync

È possibile che venga `GatewayClockOutOfSync` visualizzato un errore quando il gateway rileva una differenza di almeno 5 minuti tra l'ora del sistema locale e l'ora riportata dai server AWS Storage Gateway. I problemi di sincronizzazione dell'orologio possono influire negativamente sulla connettività tra il gateway e. AWS Se l'orologio del gateway non è sincronizzato, potrebbero verificarsi errori di I/O per le connessioni NFS e SMB e gli utenti SMB potrebbero riscontrare errori di autenticazione.

Per risolvere un errore GatewayClockOutOfSync

- Verificare la configurazione di rete tra il gateway e il server NTP. Per ulteriori informazioni sulla sincronizzazione dell'ora della macchina virtuale del gateway e sull'aggiornamento della configurazione del server NTP, vedere Configurazione di un server Network Time Protocol (NTP) per il gateway Configurazione di un server NTP) per il gateway.

Errore: InaccessibleStorageClass

Puoi ricevere un `InaccessibleStorageClass` errore quando un oggetto viene spostato dalla classe di storage Amazon S3 Standard.

Il tuo File Gateway di solito riscontra questo errore quando tenta di caricare o leggere un oggetto dal bucket Amazon S3. In genere, questo errore indica che l'oggetto è stato spostato in Amazon Glacier e si trova nella classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Il tuo S3 File Gateway può generare un rapporto sulla cache che elenca tutti i file nella cache del gateway che attualmente non riescono a caricare su Amazon S3 a causa di questo errore. Le informazioni contenute in questo rapporto possono aiutarti a risolvere i problemi relativi Supporto al gateway, ad Amazon S3 o alla configurazione IAM. Per ulteriori informazioni, consulta Creare un rapporto sulla cache.

Per risolvere un InaccessibleStorageClass errore

- Ripristina l'oggetto dalla classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive alla classe di storage originale in S3.

Se ripristini l'oggetto nel bucket S3 per correggere un errore di caricamento, alla fine il file viene caricato. Se ripristinate l'oggetto per correggere un errore di lettura, il client SMB o NFS di File Gateway può quindi leggere il file.

Errore: InvalidObjectState

Puoi ricevere un `InvalidObjectState` errore quando un writer diverso dal File Gateway specificato modifica il file specificato nel bucket Amazon S3 specificato. Di conseguenza, lo stato del file per File Gateway non corrisponde al suo stato in Amazon S3. Eventuali caricamenti successivi del file su Amazon S3 o il recupero del file da Amazon S3 non riescono.

Il tuo S3 File Gateway può generare un rapporto sulla cache che elenca tutti i file nella cache del gateway che attualmente non riescono a caricare su Amazon S3 a causa di questo errore. Le informazioni contenute in questo rapporto possono aiutarti a risolvere i problemi relativi Supporto al gateway, ad Amazon S3 o alla configurazione IAM. Per ulteriori informazioni, consulta Creare un rapporto sulla cache.

Per risolvere un InvalidObjectState errore

Se l'operazione che modifica il file è `S3Upload` o`S3GetObject`, procedi come segue:

1. Salvate la copia più recente del file nel file system locale del client SMB o NFS (questa copia del file è necessaria nel passaggio 4). Se la versione del file in Amazon S3 è la più recente, scarica quella versione. Puoi farlo usando Console di gestione AWS o AWS CLI.
2. Elimina il file in Amazon S3 utilizzando o. Console di gestione AWS AWS CLI
3. Elimina il file da File Gateway utilizzando il client SMB o NFS.
4. Copia la versione più recente del file salvato nella fase 1 su Amazon S3 utilizzando il tuo client SMB o NFS. Fatelo tramite il vostro File Gateway.

Errore: ObjectMissing

È possibile che venga `ObjectMissing` visualizzato un errore quando un writer diverso dal File Gateway specificato elimina il file specificato dal bucket S3. Tutti i caricamenti successivi su Amazon S3 o i recuperi da Amazon S3 per l'oggetto hanno esito negativo.

Il tuo S3 File Gateway può generare un rapporto sulla cache che elenca tutti i file nella cache del gateway che attualmente non riescono a caricare su Amazon S3 a causa di questo errore. Le

informazioni contenute in questo rapporto possono aiutarti a risolvere i problemi relativi Supporto al gateway, ad Amazon S3 o alla configurazione IAM. Per ulteriori informazioni, consulta Creare un rapporto sulla cache.

Per risolvere un ObjectMissing errore

Se l'operazione che modifica il file è `S3Upload` o`S3GetObject`, procedi come segue:

1. Salvate la copia più recente del file nel file system locale del client SMB o NFS (questa copia del file è necessaria nel passaggio 3).
2. Eliminare il file dal File Gateway utilizzando il client SMB o NFS.
3. Copia la versione più recente del file che hai salvato nel passaggio 1 utilizzando il tuo client SMB o NFS. Fatelo tramite File Gateway.

Errore: RoleTrustRelationshipInvalid

Si ottiene questo errore quando il ruolo IAM per una condivisione di file ha una relazione di trust IAM configurata in modo errato (ovvero, il ruolo IAM non si fida del principale Storage Gateway denominato`storagegateway.amazonaws.com`). Di conseguenza, File Gateway non sarebbe in grado di ottenere le credenziali per eseguire alcuna operazione sul bucket S3 che supporta la condivisione di file.

Per risolvere un errore RoleTrustRelationshipInvalid

- Utilizza la console IAM o l'API IAM per includerla `storagegateway.amazonaws.com` come principale considerata affidabile dalla tua condivisione di file IAMrole. Per informazioni sul ruolo IAM, consulta Tutorial: delega l'accesso tra AWS account utilizzando i ruoli IAM.

Errore: S3 AccessDenied

Puoi ricevere un `S3AccessDenied` errore per il ruolo Amazon S3 bucket access AWS Identity and Access Management (IAM) di una condivisione di file. In questo caso, il ruolo IAM di accesso al bucket S3 specificato `roleArn` nell'errore non consente l'operazione in questione. L'operazione non è consentita a causa delle autorizzazioni per gli oggetti nella directory specificata dal prefisso Amazon S3.

Il tuo S3 File Gateway può generare un rapporto sulla cache che elenca tutti i file nella cache del gateway che attualmente non riescono a caricare su Amazon S3 a causa di questo errore. Le

informazioni contenute in questo rapporto possono aiutarti a risolvere i problemi relativi Supporto al gateway, ad Amazon S3 o alla configurazione IAM. Per ulteriori informazioni, consulta Creare un rapporto sulla cache.

Per risolvere un errore S3 AccessDenied

- Modifica la policy di accesso di Amazon S3 allegata al `roleArn` log di integrità di File Gateway per consentire le autorizzazioni per il funzionamento di Amazon S3. Assicurati che la policy di accesso consenta l'autorizzazione per l'operazione che ha causato l'errore. Inoltre, consenti l'autorizzazione per la directory specificata nel registro per `prefix`. Per informazioni sulle autorizzazioni di Amazon S3, consulta Specificare le autorizzazioni in una politica nella Guida per l'utente di Amazon Simple Storage Service.

  Queste operazioni possono causare un errore `S3AccessDenied`.

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

Errore: DroppedNotifications

È possibile che venga visualizzato un `DroppedNotifications` errore anziché altri tipi di voci di CloudWatch registro previsti quando lo spazio di archiviazione libero sul disco principale del gateway è inferiore a 1 GB o se vengono generate più di 100 notifiche sanitarie entro un intervallo di 1 minuto. In queste circostanze, il gateway interrompe la generazione di notifiche di CloudWatch registro dettagliate come misura precauzionale.

Per risolvere un DroppedNotifications errore

1. Controlla la `Root Disk Usage` metrica nella scheda Monitoraggio del gateway nella console di Storage Gateway per determinare se lo spazio disponibile su disco root si sta esaurendo.
2. Aumenta le dimensioni del disco di archiviazione principale del gateway se lo spazio disponibile è inferiore a 1 GB. Per istruzioni, consulta la documentazione dell'hypervisor della macchina virtuale.

Per aumentare le dimensioni del disco root per i EC2 gateway Amazon, consulta Richiedere modifiche ai volumi EBS nella Amazon Elastic Compute Cloud User Guide.

> **Note**
>
> Non è possibile aumentare la dimensione del disco root per lo AWS Storage Gateway Hardware Appliance.

3. Riavviare il gateway.

Notifica: HardReboot

Puoi ricevere una notifica `HardReboot` quando la VM del gateway viene riavviata in modo imprevisto. Questo riavvio può essere dovuto a mancanza di alimentazione, a un guasto hardware o a un altro evento. Per i VMware gateway, un ripristino da parte di vSphere High Availability Application Monitoring può causare questo evento.

Quando il gateway funziona in un ambiente di questo tipo, verifica la presenza della `HealthCheckFailure` notifica e consulta il registro VMware degli eventi per la macchina virtuale.

Notifica: riavvio

Puoi ricevere una notifica di riavvio quando la VM del gateway viene riavviata. Puoi riavviare una macchina virtuale gateway utilizzando la console di gestione VM Hypervisor o la console Storage Gateway. È inoltre possibile riavviare utilizzando il software del gateway durante il ciclo di manutenzione del gateway.

Se il riavvio viene eseguito entro 10 minuti dall'ora di avvio della manutenzione configurata del gateway, probabilmente è un evento normale e non un'indicazione di problema. Se il riavvio è stato eseguito al di fuori della finestra di manutenzione in modo significativo, verifica se il gateway è stato riavviato manualmente.

Risoluzione dei problemi: le scansioni di sicurezza mostrano porte NFS aperte

Alcune porte NFS sono abilitate per impostazione predefinita, anche sui gateway utilizzati solo con le condivisioni di file SMB. Se si utilizza un software di sicurezza di terze parti come Qualys per

scansionare la rete in cui è distribuito File Gateway, i risultati della scansione potrebbero segnalare queste porte NFS aperte come una potenziale vulnerabilità di sicurezza. Se utilizzate il gateway solo con condivisioni di file SMB e desiderate disabilitare le porte NFS non utilizzate per motivi di sicurezza, utilizzate la seguente procedura:

Per disabilitare le porte NFS su un File Gateway:

1. Accedere al prompt dei comandi della console locale del gateway utilizzando la procedura descritta in. Esecuzione di comandi Storage Gateway sulla console locale
2. Immettete i seguenti comandi per disabilitare il traffico NFS:

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

3. Immettete il seguente comando per confermare che le porte NFS bloccate vengano visualizzate nelle tabelle IP:

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

Risoluzione dei problemi: utilizzo CloudWatch delle metriche

Di seguito puoi trovare informazioni sulle azioni per risolvere i problemi utilizzando i CloudWatch parametri di Amazon con Storage Gateway.

Argomenti

- Il gateway reagisce lentamente durante la navigazione nelle directory
- Il tuo gateway non risponde
- Il tuo gateway è lento nel trasferimento dei dati su Amazon S3
- Il tuo gateway sta eseguendo più operazioni Amazon S3 del previsto
- Non vedi file nel tuo bucket Amazon S3
- Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway

Il gateway reagisce lentamente durante la navigazione nelle directory

Se File Gateway reagisce lentamente quando esegui il ls comando o sfogli le directory, controlla le `IndexFetch` metriche and: `IndexEviction` CloudWatch

- Se la `IndexFetch` metrica è maggiore di 0 quando esegui un `ls` comando o sfogli le directory, File Gateway si è avviato senza informazioni sul contenuto della directory interessata e ha dovuto accedere ad Amazon FSx S3 Windows File Server. Gli sforzi successivi per elencare i contenuti di tale directory dovrebbero avvenire più velocemente.
- Se la `IndexEviction` metrica è maggiore di 0, significa che File Gateway ha raggiunto il limite di ciò che può gestire nella cache in quel momento. In questo caso, File Gateway deve liberare dello spazio di archiviazione dalla directory a cui si accede meno di recente per elencare una nuova directory. Se ciò si verifica frequentemente e si verifica un impatto sulle prestazioni, contattateci Supporto.

  Supporto Parla del contenuto del bucket S3 correlato e dei consigli per migliorare le prestazioni in base al tuo caso d'uso.

Il tuo gateway non risponde

Se il File Gateway non risponde, procedi come segue:

- Se di recente è stato eseguito un riavvio o aggiornamento software, controlla il parametro `IOWaitPercent`. Questa metrica mostra la percentuale di tempo in cui la CPU è inattiva quando c'è una richiesta di disco in sospeso. I/O In alcuni casi, questo valore potrebbe essere elevato (10 o maggiore) e potrebbe essere aumentato dopo il riavvio o l'aggiornamento del server. In questi casi, File Gateway potrebbe essere bloccato da un disco root lento mentre ricostruisce la cache degli indici in RAM. Puoi risolvere questo problema utilizzando un disco fisico più veloce per il disco root.
- Se la `MemUsedBytes` metrica è uguale o quasi uguale alla `MemTotalBytes` metrica, significa che File Gateway sta esaurendo la RAM disponibile. Assicurati che File Gateway disponga almeno della RAM minima richiesta. Se lo è già, valuta la possibilità di aggiungere più RAM al File Gateway in base al carico di lavoro e al caso d'uso.

  Se la condivisione file è SMB, il problema potrebbe anche essere dovuto al numero di client SMB connessi alla condivisione file. Controlla il parametro `SMBV(1/2/3)Sessions` per vedere il numero di client connessi in un dato momento. Se ci sono molti client connessi, potrebbe essere necessario aggiungere più RAM al File Gateway.

Il tuo gateway è lento nel trasferimento dei dati su Amazon S3

Se il tuo File Gateway trasferisce lentamente i dati su Amazon S3, procedi come segue:

- Se il `CachePercentDirty` parametro è pari o superiore a 80, File Gateway scrive i dati su disco più velocemente di quanto possa caricarli su Amazon S3. Valuta la possibilità di aumentare la larghezza di banda per il caricamento da File Gateway, aggiungere uno o più dischi di cache o rallentare le scritture dei client.
- Se la `CachePercentDirty` metrica è bassa, controllala. `IoWaitPercent` Se `IoWaitPercent` è maggiore di 10, il File Gateway potrebbe essere ostacolato dalla velocità del disco di cache locale. Consigliamo dischi SSD (Solid State Drive) locali per la cache, preferibilmente NVM Express (). NVMe Se questi dischi non sono disponibili, prova a utilizzare più dischi di cache da dischi fisici separati per migliorare le prestazioni.
- Se`S3PutObjectRequestTime`, o `S3GetObjectRequestTime` sono`S3UploadPartRequestTime`, sono alti, potrebbe esserci un collo di bottiglia nella rete. Prova ad analizzare la tua rete per verificare che il gateway abbia la larghezza di banda prevista.

Il tuo gateway sta eseguendo più operazioni Amazon S3 del previsto

Se il tuo File Gateway esegue più operazioni Amazon S3 del previsto, controlla la `FilesRenamed` metrica. Le operazioni di ridenominazione sono costose da eseguire in Amazon S3. Ottimizza il flusso di lavoro per ridurre al minimo il numero di operazioni di ridenominazione.

Non vedi file nel tuo bucket Amazon S3

Se noti che i file sul gateway non si riflettono nel bucket Amazon S3, controlla la metrica. `FilesFailingUpload` Se la metrica riporta che alcuni file non vengono caricati correttamente, controlla le tue notifiche sanitarie. Quando i file non vengono caricati, il gateway genera una notifica sanitaria contenente maggiori dettagli sul problema.

Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway

Se il processo di backup di File Gateway non riesce o si verificano errori durante la scrittura su File Gateway, effettuate le seguenti operazioni:

- Se la `CachePercentDirty` metrica è pari o superiore al 90 percento, File Gateway non può accettare nuove scritture su disco perché lo spazio disponibile sul disco della cache non è sufficiente. Per vedere la velocità di caricamento di File Gateway su Amazon FSx Server, visualizza `CloudBytesUploaded` la metrica. Confronta questa metrica con la `WriteBytes` metrica, che mostra la velocità con cui il client scrive file sul tuo File Gateway. Se il client SMB sta scrivendo sul tuo File Gateway più velocemente di quanto possa caricare su Amazon FSx Server, aggiungi altri dischi di cache per coprire al minimo le dimensioni del processo di backup. In alternativa, aumenta la larghezza di banda di caricamento.
- Se una copia di file di grandi dimensioni, ad esempio un processo di backup, fallisce ma la `CachePercentDirty` metrica è inferiore all'80%, File Gateway potrebbe raggiungere un timeout della sessione lato client. Per SMB, è possibile aumentare questo timeout utilizzando il comando. PowerShell `Set-SmbClientConfiguration -SessionTimeout 300` L'esecuzione di questo comando imposta il timeout su 300 secondi.

  Per NFS, assicurati che il client sia montato utilizzando un hard mount anziché un soft mount.

Risoluzione dei problemi: problemi di condivisione dei file

Di seguito è spiegato cosa fare se si verificano problemi imprevisti nella condivisione file.

Argomenti

- La condivisione di file è bloccata nello stato CREATING
- Non puoi creare una condivisione di file
- Le condivisioni di file SMB non consentono più metodi di accesso diversi
- Più condivisioni di file non possono scrivere sul bucket S3 mappato
- Notifica per il gruppo di log eliminato quando si utilizzano i log di controllo
- Impossibile caricare file nel bucket S3
- Non riesco a modificare la crittografia predefinita per utilizzare SSE-KMS per crittografare gli oggetti archiviati nel mio bucket S3
- Le modifiche apportate direttamente in un bucket S3 con il controllo delle versioni degli oggetti attivato possono influire su ciò che vedi nella condivisione di file
- Quando si scrive su un bucket S3 con il controllo delle versioni attivato, Amazon S3 File Gateway può creare più versioni di oggetti Amazon S3
- Le modifiche a un bucket S3 non si riflettono in Storage Gateway
- Le autorizzazioni ACL non funzionano come previsto
- Le prestazioni del gateway sono diminuite dopo l'esecuzione di un'operazione ricorsiva

La condivisione di file è bloccata nello stato CREATING

Non appena la configuri, alla condivisione file viene assegnato lo stato CREATING (CREAZIONE IN CORSO) che diventa AVAILABLE (DISPONIBILE) solo al termine della creazione. Se la condivisione file si blocca allo stato CREATING (CREAZIONE IN CORSO), occorre procedere come segue:

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Assicurati che il bucket S3 su cui hai mappato la condivisione di file esista. In caso contrario, crearlo. Una volta creato il bucket, lo stato della condivisione file passa a AVAILABLE (DISPONIBILE). Per informazioni su come creare un bucket S3, consulta Create a bucket nella Amazon Simple Storage Service User Guide.
3. Assicurati che il nome del bucket sia conforme alle regole per la denominazione dei bucket in Amazon S3. Per ulteriori informazioni, consulta le Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

> **Note**
>
> S3 File Gateway non supporta i bucket Amazon S3 con periodi `.` () nel nome del bucket.

4. Assicurati che il ruolo IAM che hai usato per accedere al bucket S3 disponga delle autorizzazioni corrette e verifica che il bucket S3 sia elencato come risorsa nella policy IAM. Per ulteriori informazioni, consulta Concessione dell'accesso a un bucket Amazon S3.

Non puoi creare una condivisione di file

1. Se non riesci a creare una condivisione di file perché la condivisione di file è bloccata nello stato CREATING, verifica che il bucket S3 su cui hai mappato la condivisione di file esista. Per informazioni su come fare, consulta il paragrafo precedente, La condivisione di file è bloccata nello stato CREATING.
2. Se il bucket S3 esiste, verifica che AWS Security Token Service sia attivato nella regione in cui stai creando la condivisione di file. Se un token di sicurezza non è attivo, dovresti attivarlo. Per informazioni su come attivare un token utilizzando AWS Security Token Service, consulta Attivazione e disattivazione di AWS STS in una AWS regione nella Guida per l'utente IAM.

Le condivisioni di file SMB non consentono più metodi di accesso diversi

Le condivisioni di file SMB hanno le seguenti restrizioni:

1. Quando lo stesso client tenta di montare sia una condivisione file Active Directory che una condivisione SMB con accesso guest viene visualizzato il seguente messaggio di errore: `Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Un utente di Windows non può essere connesso a due condivisioni di file SMB con accesso guest e potrebbe essere disconnesso quando viene stabilita una nuova connessione con accesso guest.
3. Un client di Windows non è in grado di montare insieme una condivisione file Active Directory e una condivisione SMB con accesso guest esportate dallo stesso gateway.

Più condivisioni di file non possono scrivere sul bucket S3 mappato

Non è consigliabile configurare il bucket S3 per consentire la scrittura di più condivisioni di file su un unico bucket S3. Tale approccio, infatti, è in grado di determinare risultati imprevisti.

Al contrario, è bene consentire a un'unica condivisione file di scrivere su ciascun bucket S3. Per permettere al solo ruolo associato alla tua condivisione file di scrivere sul bucket, puoi creare una policy del bucket. Per ulteriori informazioni, consulta Best Practices for File Gateway.

Notifica per il gruppo di log eliminato quando si utilizzano i log di controllo

Se il gruppo di log non esiste, l'utente può selezionare il collegamento al gruppo di log sotto il messaggio per creare un nuovo gruppo di log o utilizzare un gruppo di log esistente da utilizzare come destinazione per i log di controllo

Impossibile caricare file nel bucket S3

Se non riesci a caricare file nel tuo bucket S3, procedi come segue:

1. Assicurati di aver concesso l'accesso richiesto ad Amazon S3 File Gateway per caricare file nel tuo bucket S3. Per ulteriori informazioni, consulta Concessione dell'accesso a un bucket Amazon S3.
2. Verificare che il ruolo che ha creato il bucket sia autorizzato a scrivere nel bucket S3. Per ulteriori informazioni, consulta Best Practices for File Gateway.
3. Se il tuo File Gateway utilizza SSE-KMS o DSSE-KMS per la crittografia, assicurati che il ruolo IAM associato alla condivisione di file includa le autorizzazioni KMS:Encrypt, KMS:Decrypt, kms: *, kms: e kms:. ReEncrypt GenerateDataKey DescribeKey Per ulteriori informazioni, consulta Using Identity-Based Policies (IAM Policies) for Storage Gateway.

Non riesco a modificare la crittografia predefinita per utilizzare SSE-KMS per crittografare gli oggetti archiviati nel mio bucket S3

Se modifichi la crittografia predefinita e rendi SSE-KMS (crittografia lato server con chiavi AWS KMS gestite) l'impostazione predefinita per il tuo bucket S3, gli oggetti archiviati da Amazon S3 File Gateway nel bucket non vengono crittografati con SSE-KMS. Per impostazione predefinita, un S3 File Gateway utilizza la crittografia lato server gestita con Amazon S3 (SSE-S3) quando scrive dati in un bucket S3. Modificare l'impostazione predefinita non modificherà automaticamente la crittografia.

Per modificare la crittografia per utilizzare SSE-KMS con la tua chiave, devi attivare la crittografia SSE-KMS. AWS KMS A tale scopo, ti basta fornire l'Amazon Resource Name (ARN) della chiave KMS quando crei la condivisione file. Puoi anche aggiornare le impostazioni KMS per la condivisione file utilizzando l'operazione API `UpdateNFSFileShare` o `UpdateSMBFileShare`. Questo aggiornamento si applica agli oggetti archiviati nei bucket S3 dopo l'aggiornamento. Per ulteriori informazioni, consulta Crittografia dei dati utilizzando AWS KMS.

Le modifiche apportate direttamente in un bucket S3 con il controllo delle versioni degli oggetti attivato possono influire su ciò che vedi nella condivisione di file

Se il bucket S3 contiene oggetti scritti da un altro client, la visualizzazione del bucket S3 potrebbe non essere up-to-date il risultato del controllo delle versioni degli oggetti del bucket S3. Prima di esaminare i file d'interesse, occorre aggiornare la cache.

La funzione Versioni multiple degli oggetti è una funzione facoltativa dei bucket S3 che consente di preservare i dati memorizzando più copie di un oggetto con lo stesso nome. A ciascuna copia è assegnato un valore ID univoco, ad esempio `file1.jpg`: `ID="xxx"` e `file1.jpg`: `ID="yyy"`. Il numero di oggetti con lo stesso nome e la loro durata sono controllati dalle politiche del ciclo di vita di Amazon S3. Per ulteriori dettagli su questi concetti di Amazon S3, consulta Using versioning and Object Lifecycle Management nella Amazon S3 Developer Guide.

Un oggetto con versione eliminato acquisisce il contrassegno di eliminazione, ma viene conservato. Solo il proprietario del bucket S3 può eliminare definitivamente un oggetto con la funzione Versioni multiple attiva.

In S3 File Gateway, i file mostrati sono le versioni più recenti degli oggetti in un bucket S3 al momento in cui l'oggetto è stato recuperato o la cache è stata aggiornata. Gli S3 File Gateway ignorano le versioni precedenti o gli oggetti contrassegnati per l'eliminazione. Quando si legge un file, vengono visualizzati i dati della versione più recente. Quando scrivi un file nella condivisione di file, S3 File Gateway crea una nuova versione di un oggetto denominato con le modifiche apportate, e quella versione diventa la versione più recente.

S3 File Gateway continua a leggere dalla versione precedente e gli aggiornamenti che apporti si basano sulla versione precedente nel caso in cui venga aggiunta una nuova versione al bucket S3 al di fuori dell'applicazione. Per leggere la versione più recente di un oggetto, utilizza l'azione RefreshCacheAPI o aggiorna dalla console come descritto in. Aggiornamento della cache degli oggetti del bucket Amazon S3

> **Important**
>
> Non è consigliabile scrivere oggetti o file nel bucket S3 File Gateway S3 dall'esterno della condivisione di file.

Quando si scrive su un bucket S3 con il controllo delle versioni attivato, Amazon S3 File Gateway può creare più versioni di oggetti Amazon S3

Con il controllo delle versioni degli oggetti attivato, potresti avere più versioni di un oggetto creato in Amazon S3 per ogni aggiornamento di un file dal tuo client NFS o SMB. Ecco alcuni scenari che possono comportare la creazione di più versioni di un oggetto nel bucket S3:

- Quando un file viene modificato in Amazon S3 File Gateway da un client NFS o SMB dopo che è stato caricato su Amazon S3, S3 File Gateway carica i dati nuovi o modificati anziché caricare l'intero file. La modifica del file comporta la creazione di una nuova versione dell'oggetto Amazon S3.
- Quando un file viene scritto su S3 File Gateway da un client NFS o SMB, S3 File Gateway carica i dati del file su Amazon S3 seguiti dai relativi metadati (proprietà, timestamp, ecc.). Il caricamento dei dati del file crea un oggetto Amazon S3 e il caricamento dei metadati per il file aggiorna i metadati per l'oggetto Amazon S3. Questo processo crea un'altra versione dell'oggetto, ottenendo due versioni di un oggetto.
- Quando S3 File Gateway carica file di grandi dimensioni, potrebbe essere necessario caricare porzioni più piccole del file prima che il client abbia finito di scrivere sul File Gateway. Alcuni motivi includono la necessità di liberare spazio nella cache o un'elevata velocità di scrittura su un file. Ciò può comportare più versioni di un oggetto nel bucket S3.

È necessario monitorare il bucket S3 per determinare quante versioni di un oggetto esistono prima di configurare le politiche del ciclo di vita per spostare gli oggetti in classi di storage diverse. È necessario configurare la scadenza del ciclo di vita per le versioni precedenti per ridurre al minimo il numero di versioni di un oggetto nel bucket S3. L'uso della replica Same-Region (SRR) o della replica Cross-Region (CRR) tra i bucket S3 aumenterà lo storage utilizzato. Per ulteriori informazioni sulla replica, vedere Replica.

> **Important**
>
> Non configurate la replica tra i bucket S3 prima di aver compreso la quantità di storage utilizzata quando viene attivato il controllo delle versioni degli oggetti.

L'uso di bucket S3 con versioni diverse può aumentare notevolmente la quantità di storage in Amazon S3 perché ogni modifica a un file crea una nuova versione dell'oggetto S3. Per impostazione predefinita, Amazon S3 continua a memorizzare tutte queste versioni a meno che non si crei specificamente una policy per ignorare questo comportamento e limitare il numero di versioni che vengono conservate. Se noti un utilizzo insolitamente elevato dello storage con il controllo delle versioni degli oggetti attivato, verifica che le politiche di storage siano impostate in modo appropriato. L'utilizzo della funzione Versioni multiple degli oggetti può provocare, inoltre, l'incremento del numero di risposte `HTTP 503-slow down` alle richieste del browser.

Se attivi il controllo delle versioni degli oggetti dopo aver installato un S3 File Gateway, tutti gli oggetti unici vengono mantenuti (`ID="NULL"`) e puoi vederli tutti nel file system. Alle nuove versioni degli oggetti viene assegnato un ID univoco (le versioni precedenti vengono comunque conservate). Nel file system NFS viene visualizzata solo l'ultima versione dell'oggetto in base al suo time stamp.

Dopo aver attivato il controllo delle versioni degli oggetti, non è possibile ripristinare lo stato senza versioni del bucket S3. Tuttavia, si può sospendere la funzione. In seguito alla sospensione, a un nuovo oggetto viene assegnato un ID. In presenza di un oggetto con lo stesso nome e un valore `ID="NULL"`, la versione meno recente viene sovrascritta. Eventuali versioni contenenti un ID diverso da `NULL`, tuttavia, restano disponibili. I time stamp identificano il nuovo oggetto come quello attuale, nonché l'unico da visualizzare nel file system NFS.

Le modifiche a un bucket S3 non si riflettono in Storage Gateway

Storage Gateway aggiorna automaticamente la cache di condivisione dei file quando si scrivono file nella cache localmente utilizzando la condivisione di file. Tuttavia, Storage Gateway non aggiorna automaticamente la cache quando carichi un file direttamente su Amazon S3. Quando si esegue questa operazione, è necessario eseguire un'`RefreshCache`operazione per visualizzare le modifiche sulla condivisione di file. Se si dispone di più di una condivisione di file, è necessario eseguire l'`RefreshCache`operazione su ciascuna condivisione di file.

È possibile aggiornare la cache utilizzando la console Storage Gateway e AWS Command Line Interface (AWS CLI):

- Per aggiornare la cache utilizzando la console Storage Gateway, consulta Refreshing objects in your Amazon S3 bucket.
- Per aggiornare la cache utilizzando: AWS CLI
  1. Esegui il comando `aws storagegateway list-file-shares`
  2. Copia l'Amazon Resource Number (ARN) della condivisione di file con la cache che desideri aggiornare.
  3. Esegui il `refresh-cache` comando con il tuo ARN come valore per: `--file-share-arn`

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

Per automatizzare l'`RefreshCache`operazione, vedi Come posso automatizzare l' RefreshCache operazione su Storage Gateway?

Le autorizzazioni ACL non funzionano come previsto

Se le autorizzazioni della lista di controllo accessi (ACL) non funzionano come previsto con la tua condivisione di file SMB, è possibile eseguire un test.

Per eseguire questa operazione, testa prima le autorizzazioni su un server di file di Microsoft Windows o in una condivisione locale di file Windows. Quindi confronta il comportamento con la condivisione di file del gateway.

Le prestazioni del gateway sono diminuite dopo l'esecuzione di un'operazione ricorsiva

In alcuni casi, è possibile eseguire un'operazione ricorsiva, ad esempio rinominare una directory o attivare l'ereditarietà per un ACL, e forzarla verso il basso nell'albero. Se si esegue questa operazione, S3 File Gateway applica l'operazione in modo ricorsivo a tutti gli oggetti nella condivisione di file.

Ad esempio, supponiamo di applicare l'ereditarietà agli oggetti esistenti in un bucket S3. Il tuo S3 File Gateway applica in modo ricorsivo l'ereditarietà a tutti gli oggetti nel bucket. Tali operazioni possono provocare il peggioramento delle prestazioni del gateway.

Notifiche di stato della disponibilità elevata

Quando si esegue il gateway sulla piattaforma VMware vSphere High Availability (HA), è possibile ricevere notifiche sullo stato. Per ulteriori informazioni sulle notifiche sullo stato, consulta Risoluzione dei problemi: problemi di alta disponibilità.

Risoluzione dei problemi: problemi di alta disponibilità

Di seguito sono riportate le informazioni sulle azioni da intraprendere in caso di problemi di disponibilità.

Argomenti

- Notifiche di stato
- Parametri

Notifiche di stato

Quando esegui il gateway su VMware vSphere HA, tutti i gateway generano le seguenti notifiche di integrità al gruppo di log Amazon CloudWatch configurato. Queste notifiche vengono inserite in un flusso di log chiamato `AvailabilityMonitor`.

Argomenti

- Notifica: riavvio
- Notifica: HardReboot
- Notifica: HealthCheckFailure
- Notifica: AvailabilityMonitorTest

Notifica: riavvio

Puoi ricevere una notifica di riavvio quando la VM del gateway viene riavviata. Puoi riavviare una macchina virtuale gateway utilizzando la console di gestione VM Hypervisor o la console Storage Gateway. È inoltre possibile riavviare utilizzando il software del gateway durante il ciclo di manutenzione del gateway.

Operazione da eseguire

Se il riavvio viene eseguito entro 10 minuti dall'ora di avvio della manutenzione configurata del gateway, probabilmente si tratta di un evento normale e non un'indicazione di problema. Se il riavvio è stato eseguito al di fuori della finestra di manutenzione in modo significativo, verifica se il gateway è stato riavviato manualmente.

Notifica: HardReboot

Puoi ricevere una notifica `HardReboot` quando la VM del gateway viene riavviata in modo imprevisto. Questo riavvio può essere dovuto a mancanza di alimentazione, a un guasto hardware o a un altro evento. Per i VMware gateway, un ripristino da parte di vSphere High Availability Application Monitoring può causare questo evento.

Operazione da eseguire

Quando il gateway funziona in un ambiente di questo tipo, verifica la presenza della `HealthCheckFailure` notifica e consulta il registro VMware degli eventi per la macchina virtuale.

Notifica: HealthCheckFailure

Per un gateway su VMware vSphere HA, è possibile ricevere una `HealthCheckFailure` notifica quando un controllo di integrità fallisce e viene richiesto il riavvio della macchina virtuale. Questo evento si verifica anche durante un test per monitorare la disponibilità, indicato da una notifica `AvailabilityMonitorTest`. In questo caso, la notifica `HealthCheckFailure` è prevista.

> **Note**
>
> Questa notifica è valida solo per i VMware gateway.

Operazione da eseguire

Se questo evento si verifica ripetutamente senza notifica `AvailabilityMonitorTest`, verifica la presenza di problemi nell'infrastruttura VM (storage, memoria e così via). Se hai bisogno di ulteriore assistenza, contatta Supporto.

Notifica: AvailabilityMonitorTest

Per un gateway su VMware vSphere HA, è possibile ricevere una `AvailabilityMonitorTest` notifica quando si esegue un test del sistema di monitoraggio della disponibilità e delle applicazioni in. VMware

Parametri

Il parametro `AvailabilityNotifications` è disponibile in tutti i gateway. Questo parametro è il conteggio del numero di notifiche di stato relative alla disponibilità generate dal gateway. Utilizza la statistica `Sum` per verificare se il gateway sta riscontrando eventi correlati alla disponibilità. Consultate il gruppo di CloudWatch log configurato per i dettagli sugli eventi.

Le migliori pratiche per File Gateway

Questa sezione contiene gli argomenti seguenti, che forniscono informazioni sulle migliori pratiche per lavorare con gateway, condivisioni di file, bucket e dati. Ti consigliamo di acquisire familiarità con le informazioni descritte in questa sezione e di provare a seguire queste linee guida per evitare problemi con il tuo. Gateway di archiviazione AWS Per ulteriori indicazioni sulla diagnosi e la risoluzione dei problemi più comuni che potresti riscontrare durante la distribuzione, consulta. Risoluzione dei problemi relativi all'implementazione dello Storage Gateway

Argomenti

- Migliori pratiche: ripristino dei dati
- Migliori pratiche: gestione dei caricamenti in più parti
- Procedure consigliate: decomprimi i file compressi localmente prima di copiarli su un gateway
- Conserva gli attributi dei file durante la copia dei dati da Windows Server
- Procedure consigliate: dimensionamento corretto dei dischi di cache
- Utilizzo di più condivisioni di file e bucket Amazon S3
- Pulisci le risorse non necessarie

Migliori pratiche: ripristino dei dati

Sebbene improbabile, si potrebbe verificare un errore irreversibile del gateway. Tale errore può verificarsi nella macchina virtuale (VM), nel gateway stesso, nello storage locale o in altre posizioni. Se si verifica un errore, è consigliabile seguire le istruzioni nella sezione appropriata di seguito per ripristinare i dati.

> **Important**
>
> Storage Gateway non supporta il ripristino di una macchina virtuale gateway da uno snapshot creato dall'hypervisor o dall'Amazon Amazon EC2 Machine Image (AMI). Se la macchina virtuale del gateway non funziona correttamente, attiva un nuovo gateway e ripristina i dati in tale gateway in base alle istruzioni seguenti.

Ripristino da un arresto imprevisto della macchina virtuale

Se la macchina virtuale si arresta in modo imprevisto, ad esempio in caso di interruzione dell'alimentazione, il gateway diventa irraggiungibile. Quando l'alimentazione e la connettività di rete vengono ripristinate, il gateway diventa raggiungibile e inizia a funzionare normalmente. Di seguito sono elencate alcune fasi da seguire per ripristinare i dati:

- Se un'interruzione provoca problemi di connettività di rete, è possibile risolvere il problema. Per informazioni su come testare la connettività di rete, consulta Verifica della connettività di rete del gateway.

Ripristino dei dati da un disco della cache malfunzionante

Se nel disco della cache si verifica un errore, è consigliabile usare le opzioni seguenti per ripristinare i dati, in base alla situazione:

- Se il malfunzionamento si è verificato perché un disco della cache è stato rimosso dall'host, arresta il gateway, aggiungi di nuovo il disco e riavvia il gateway.

Ripristino dei dati da un data center inaccessibile

Se il gateway o il data center diventa inaccessibile per qualche motivo, puoi ripristinare i dati su un altro gateway in un altro data center o ripristinarli su un gateway ospitato su un' EC2 istanza Amazon. Se non hai accesso a un altro data center, ti consigliamo di creare il gateway su un' EC2 istanza Amazon. Le fasi da seguire dipendono dal tipo di gateway da cui vengono ripristinati i dati.

Per recuperare i dati da un File Gateway in un data center inaccessibile

Per File Gateway, mappi un nuovo al bucket Amazon S3 FSx che contiene i dati che desideri ripristinare.

1. Crea e attiva un nuovo File Gateway su un EC2 host Amazon. Per ulteriori informazioni, consulta Implementa un EC2 host Amazon predefinito per S3 File Gateway.
2. Crea un nuovo sul EC2 gateway che hai creato. Per ulteriori informazioni, consulta Creare una condivisione di file .
3. Installa il file system di condivisione sul client e mappalo al bucket S3 FSx che contiene i dati che desideri ripristinare. Per ulteriori informazioni, consulta Montare e utilizzare la condivisione di file .

Migliori pratiche: gestione dei caricamenti in più parti

Quando si trasferiscono file di grandi dimensioni, S3 File Gateway utilizza la funzionalità di caricamento multiparte di Amazon S3 per suddividere i file in parti più piccole e trasferirli in parallelo per una maggiore efficienza. Per ulteriori informazioni sul caricamento in più parti, consulta Caricamento e copia di oggetti utilizzando il caricamento multiparte nella Guida per l'utente di Amazon Simple Storage Service.

Se un caricamento in più parti non viene completato correttamente per qualsiasi motivo, il gateway in genere interrompe il trasferimento, elimina tutte le parti del file parzialmente trasferite da Amazon S3 e tenta nuovamente il trasferimento. In rari casi, ad esempio quando un guasto hardware o di rete impedisce la pulizia del gateway dopo un caricamento multiparte non riuscito, parti del file parzialmente trasferito potrebbero rimanere su Amazon S3 dove possono incorrere in costi di archiviazione.

Come best practice per ridurre al minimo i costi di storage di Amazon S3 dovuti a caricamenti multiparte incompleti, consigliamo di configurare una regola del ciclo di vita del bucket Amazon S3 che `AbortIncompleteMultipartUpload` utilizzi l'azione API per interrompere automaticamente i trasferimenti non riusciti ed eliminare le parti di file associate dopo un determinato numero di giorni. Per istruzioni, consulta Configurazione di una configurazione del ciclo di vita del bucket per eliminare caricamenti multiparte incompleti nella Guida per l'utente di Amazon Simple Storage Service.

Procedure consigliate: decomprimi i file compressi localmente prima di copiarli su un gateway

Se si tenta di decomprimere un archivio compresso contenente migliaia di file mentre è archiviato sul gateway, è possibile che si verifichino ritardi significativi legati alle prestazioni. Il processo di decompressione di un archivio che contiene un gran numero di file su qualsiasi tipo di condivisione di file di rete implica intrinsecamente un elevato volume di input/output operazioni, manipolazione della cache dei metadati, sovraccarico di rete e latenza. Inoltre, Storage Gateway non è in grado di determinare quando la decompressione di ogni file dell'archivio è terminata e può iniziare a caricare i file prima del completamento del processo, con un ulteriore impatto sulle prestazioni. Questi problemi si aggravano quando i file all'interno dell'archivio sono numerosi, ma di piccole dimensioni.

Come procedura ottimale, consigliamo di trasferire gli archivi compressi dal gateway al computer locale prima di decomprimerli. Quindi, se necessario, puoi utilizzare uno strumento come robocopy o rsync per ritrasferire i file decompressi al gateway.

Conserva gli attributi dei file durante la copia dei dati da Windows Server

È possibile copiare file su File Gateway utilizzando il `copy` comando di base di Microsoft Windows, ma per impostazione predefinita questo comando copia solo i dati dei file, omettendo determinati attributi dei file come i descrittori di sicurezza. Se i file vengono copiati sul gateway senza le corrispondenti restrizioni di sicurezza e le informazioni DACL (Discretionary Access Control List), è possibile che utenti non autorizzati possano accedervi.

Come procedura consigliata per preservare tutti gli attributi dei file e le informazioni di sicurezza durante la copia di file sul gateway su Microsoft Windows Server, si consiglia di utilizzare i `xcopy` comandi `robocopy` o, rispettivamente con i `/o` flag `/copy:DS` o. Per ulteriori informazioni, consulta robocopy e xcopy nella documentazione di riferimento dei comandi di Microsoft Windows Server.

Procedure consigliate: dimensionamento corretto dei dischi di cache

Per prestazioni ottimali, la dimensione totale della cache del disco deve essere sufficientemente grande da coprire le dimensioni del workset attivo. Per read/write carichi di lavoro misti e con elevata intensità di lettura, ciò garantisce una percentuale elevata di accessi alla cache durante le letture, il che è auspicabile. Puoi monitorarlo tramite la `CacheHitPercent` metrica per il tuo S3 File Gateway.

Per carichi di lavoro con elevati livelli di scrittura (ad esempio per il backup e l'archiviazione), S3 File Gateway memorizza nel buffer le scritture in entrata sulla cache del disco prima di copiare questi dati in modo asincrono su Amazon S3. È necessario assicurarsi di disporre di una capacità di cache sufficiente per memorizzare nel buffer i dati scritti. La `CachePercentDirty` metrica fornisce un'indicazione della percentuale di cache su disco che non è ancora stata mantenuta. AWS

Sono auspicabili valori bassi `CachePercentDirty` di. I valori costantemente vicini al 100% indicano che S3 File Gateway non è in grado di tenere il passo con la velocità del traffico di scrittura in entrata. Puoi evitarlo aumentando la capacità di cache su disco fornita o aumentando la larghezza di banda di rete dedicata disponibile da S3 File Gateway ad Amazon S3 o entrambi.

Per ulteriori informazioni sul dimensionamento del disco della cache, consulta le best practice di dimensionamento della cache di Amazon S3 File Gateway sul canale ufficiale Amazon Web Services. YouTube

Utilizzo di più condivisioni di file e bucket Amazon S3

Quando configuri un singolo bucket Amazon S3 per consentire la scrittura su più gateway o condivisioni di file, i risultati possono essere imprevedibili. Puoi configurare i bucket in due modi per evitare risultati imprevedibili. Scegli il metodo di configurazione più adatto al tuo caso d'uso tra le seguenti opzioni:

- Configura i tuoi bucket S3 in modo che solo una condivisione di file possa scrivere su ogni bucket. Usa una condivisione di file diversa per scrivere su ogni bucket.

  Per fare ciò, crea una policy sui bucket S3 che neghi tutti i ruoli tranne il ruolo utilizzato per una condivisione di file specifica per inserire o eliminare oggetti nel bucket. Allega una politica simile a ciascun bucket, specificando una condivisione di file diversa da scrivere in ogni bucket.

  La seguente policy di esempio nega le autorizzazioni di scrittura del bucket S3 a tutti i ruoli ad eccezione del ruolo che ha creato il bucket. Le operazioni `s3:DeleteObject` e `s3:PutObject` vengono impedite a tutti i ruoli ad eccezione di `"TestUser"`. La policy si applica a tutti gli oggetti nel bucket `"arn:aws:s3:::amzn-s3-demo-bucket/*"`.

  JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

- Se desideri che più condivisioni di file scrivano sullo stesso bucket Amazon S3, devi impedire che le condivisioni di file tentino di scrivere sugli stessi oggetti contemporaneamente.

  A tale scopo, configura un prefisso di oggetto separato e unico per ogni condivisione di file. Ciò significa che ogni condivisione di file scrive solo su oggetti con il prefisso corrispondente e non scrive su oggetti associati alle altre condivisioni di file presenti nella distribuzione. Si configura il prefisso dell'oggetto nel campo del nome del prefisso S3 quando si crea una nuova condivisione di file.

Pulisci le risorse non necessarie

Come best practice, consigliamo di ripulire le risorse di Storage Gateway per evitare addebiti imprevisti o non necessari. Ad esempio, se hai creato un gateway come esercizio dimostrativo o come test, valuta la possibilità di eliminarlo insieme alla relativa appliance virtuale dalla distribuzione. Utilizzare la procedura seguente per ripulire le risorse.

Per eliminare risorse non necessarie

1. Se non intendi più continuare a utilizzare un gateway, eliminalo. Per ulteriori informazioni, consulta Eliminazione del gateway e rimozione delle risorse associate.
2. Eliminare la macchina virtuale Storage Gateway dall'host on-premise. Se hai creato il gateway su un' EC2istanza Amazon, interrompi l'istanza.

Risorse Storage Gateway aggiuntive

Questa sezione contiene i seguenti argomenti, che forniscono informazioni e risorse aggiuntive relative alla configurazione e all'utilizzo Gateway di archiviazione AWS:

Argomenti

- Configurazione dell'host- Scopri come distribuire e configurare un host di macchina virtuale per il tuo gateway.
- Utilizzo di Storage Gateway con VMware HA- Scopri come configurare Storage Gateway per funzionare con le funzionalità di alta disponibilità di VMware vSphere.
- Ottenere la chiave di attivazione- Scopri dove trovare la chiave di attivazione da fornire quando installi un nuovo gateway.
- Supporto per gli attributi di file- Scopri come il gateway gestisce gli attributi dei file DOS e Windows.
- Usando Direct Connect- Scopri come creare una connessione di rete dedicata tra il gateway locale e il AWS cloud.
- Autorizzazioni Active Directory- Scopri quali autorizzazioni deve avere il tuo account di servizio per poter aggiungere il gateway al tuo dominio Active Directory.
- Ottenere l'indirizzo IP per il dispositivo gateway- Scopri dove trovare l'indirizzo IP dell'host della macchina virtuale del gateway, che devi fornire quando installi un nuovo gateway.
- Comprendere le risorse e le risorse IDs- Scopri come AWS identifica le risorse e le sottorisorse create da Storage Gateway.
- Tagging delle risorse - Scopri come utilizzare i tag di metadati per classificare le risorse e renderle più facili da gestire.
- Componenti open source- Scopri gli strumenti e le licenze di terze parti utilizzati per fornire la funzionalità Storage Gateway.
- Quote- Scopri i limiti e le quote per File Gateway, incluse le limitazioni minime e massime per le condivisioni di file e i dischi di cache locali.
- Utilizzo delle classi di archiviazione- Scopri le classi di storage Amazon S3 supportate da File Gateway e cosa prendere in considerazione nella scelta di una classe di storage.
- Utilizzo dei driver Kubernetes CSI- Scopri come installare e configurare i driver CSI (Container Storage Interface) per consentire alle istanze Kubernetes di utilizzare File Gateway per lo storage.
- Modulo Terraform- Scopri come usare Terraform per distribuire File Gateway come macchina virtuale.

Implementazione e configurazione dell'host VM gateway

I seguenti argomenti forniscono informazioni sulla configurazione della piattaforma host della macchina virtuale per il gateway.

Argomenti

- Implementa un EC2 host Amazon predefinito per S3 File Gateway
- Implementa un EC2 host Amazon personalizzato per S3 File Gateway
- Modifica le opzioni dei metadati delle EC2 istanze Amazon
- Sincronizza l'ora della macchina virtuale con l'ora dell'host KVM Hyper-V o Linux
- Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware
- Configurazione degli adattatori di rete per il gateway
- Utilizzo di VMware vSphere High Availability con Storage Gateway

Implementa un EC2 host Amazon predefinito per S3 File Gateway

Questo argomento elenca i passaggi per distribuire un EC2 host Amazon utilizzando le specifiche predefinite.

Puoi distribuire e attivare un Amazon S3 File Gateway Amazon File Gateway FSx un'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'AMI (Amazon Machine Image) del Gateway di archiviazione AWS è disponibile come AMI della community.

> **Note**
>
> La community AMIs di Storage Gateway è pubblicata e completamente supportata da AWS. Come si può vedere AWS, l'editore è un fornitore verificato.

1. Per configurare l' EC2 istanza Amazon, scegli Amazon EC2 come piattaforma host nella sezione Opzioni piattaforma del flusso di lavoro. Per istruzioni sulla configurazione dell' EC2 istanza Amazon, consulta Distribuzione di un' EC2istanza Amazon per ospitare Amazon S3 File Gateway File Gateway. FSx
2. Seleziona Launch instance per aprire il modello Gateway di archiviazione AWS AMI nella EC2 console Amazon e personalizzare impostazioni aggiuntive come tipi di istanza, impostazioni di rete e Configura storage.

3. Facoltativamente, puoi selezionare Usa le impostazioni predefinite nella console Storage Gateway per distribuire EC2 un'istanza Amazon con la configurazione predefinita.

   L' EC2 istanza Amazon creata da Use default settings ha le seguenti specifiche predefinite:

   - Tipo di istanza: m5.xlarge
   - Impostazioni di rete
     - Per VPC, seleziona il VPC su cui vuoi che venga eseguita l' EC2 istanza.
     - Per Subnet, specifica la sottorete in cui deve essere avviata l' EC2istanza.

     > **Note**
     >
     > Le sottoreti VPC verranno visualizzate nel menu a discesa solo se hanno l'impostazione di assegnazione automatica dell'indirizzo IP pubblico attivata dalla console di gestione VPC.

     - Assegnazione automatica di IP pubblico: attivata
     - Un gruppo EC2 di sicurezza viene creato e associato all'istanza. EC2 Il gruppo di sicurezza presenta le seguenti regole per la porta in ingresso:

     > **Note**
     >
     > È necessario che la porta 80 sia aperta durante l'attivazione del gateway. La porta viene chiusa immediatamente dopo l'attivazione. Successivamente, è possibile accedere all' EC2istanza solo tramite le altre porte del VPC selezionato.
     > Le condivisioni di file sul gateway sono accessibili solo dagli host nello stesso VPC del gateway. Se è necessario accedere alle condivisioni di file da host esterni al VPC, è necessario aggiornare le regole del gruppo di sicurezza appropriate.
     > Puoi modificare i gruppi di sicurezza in qualsiasi momento accedendo alla pagina dei dettagli dell' EC2 istanza Amazon, selezionando Sicurezza, accedendo ai dettagli del gruppo di sicurezza e scegliendo l'ID del gruppo di sicurezza.

Porta	Protocollo	Protocollo del file system				
80	TCP	Accesso HTTP per l'attivazione				
111	TCP, UDP	NFSv3				
139	TCP, UDP	SMB				
445	TCP	SMB				
2049	TCP, UDP	NFS				
20048	TCP, UDP	NFSv3				

- Configurare l'archiviazione

Impostazioni predefinite	Volume root AMI	Cache del volume 2				
Nome dispositivo		'/dev/sdb'				
Dimensione	80 GiB	165 GiB				
Tipo di volume	gp3	gp3				

Impostazioni predefinite	Volume root AMI	Cache del volume 2				
IOPS	3000	3000				
Elimina al termine	Sì	Sì				
Crittografato	No	No				
Throughput	125	125				

Implementa un EC2 host Amazon personalizzato per S3 File Gateway

Puoi distribuire e attivare un Amazon S3 File Gateway Amazon File Gateway FSx un'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'AMI (Amazon Machine Image) del Gateway di archiviazione AWS è disponibile come AMI della community.

> **Note**
>
> La community AMIs di Storage Gateway è pubblicata e completamente supportata da AWS. Come si può vedere AWS, l'editore è un fornitore verificato.
> S3 File Gateway AMIs utilizza la seguente convenzione di denominazione. Il numero di versione aggiunto al nome AMI cambia con ogni versione rilasciata.
> `aws-storage-gateway-FILE_S3-1.25.0`

Per distribuire un' EC2 istanza Amazon per ospitare il tuo Amazon S3 File Gateway

1. Inizia la configurazione di un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, consulta Configurare un Amazon S3 File Gateway Gateway. Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come piattaforma host, quindi segui i passaggi seguenti per avviare l' EC2 istanza Amazon che ospiterà il tuo File Gateway.
2. Scegli Launch instance per aprire il modello Gateway di archiviazione AWS AMI nella EC2 console Amazon, dove puoi configurare impostazioni aggiuntive.

Usa Quicklaunch per avviare l' EC2 istanza Amazon con le impostazioni predefinite. Per ulteriori informazioni sulle specifiche predefinite di Amazon EC2 Quicklaunch, consulta Quicklaunch Configuration Specifications for Amazon EC2 Amazon. EC2

3. In Nome, inserisci un nome per l' EC2 istanza Amazon. Dopo aver distribuito l'istanza, puoi cercare questo nome per trovare l'istanza nelle pagine di elenco nella EC2 console Amazon.
4. Nella sezione Tipo di istanza, per Tipo di istanza scegli la configurazione hardware per l'istanza. La configurazione hardware deve soddisfare determinati requisiti minimi per supportare il gateway. Consigliamo di iniziare con il tipo di istanza m5.xlarge, che soddisfa i requisiti minimi di hardware per il funzionamento corretto del gateway. Per ulteriori informazioni, consulta Requisiti per i tipi di EC2 istanze Amazon.

   È possibile ridimensionare l'istanza dopo l'avvio, se necessario. Per ulteriori informazioni, consulta Ridimensionamento dell'istanza nella Amazon EC2 User Guide.

   > **Note**
   >
   > Alcuni tipi di istanze, in particolare i3 EC2, utilizzano NVMe dischi SSD. Questi possono causare problemi all'avvio o all'arresto di File Gateway; ad esempio, è possibile perdere dati dalla cache. Monitora la CloudWatch metrica di `CachePercentDirty` Amazon e avvia o arresta il sistema solo quando tale parametro lo è`0`. Per ulteriori informazioni sui parametri di monitoraggio per il gateway, consulta Metriche e dimensioni dello Storage Gateway nella CloudWatch documentazione.

5. Nella sezione Coppia di chiavi (accesso), in Nome coppia di chiavi: obbligatorio, seleziona la coppia di chiavi che desideri utilizzare per connetterti in modo sicuro alla tua istanza. Se necessario, è possibile creare una nuova coppia di chiavi. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Linux.
6. Nella sezione Impostazioni di rete, rivedi le impostazioni preconfigurate e scegli Modifica per apportare modifiche ai seguenti campi:

   a. Per VPC: obbligatorio, scegli il VPC in cui desideri avviare la tua istanza Amazon. EC2 Per ulteriori informazioni, consulta Come funziona Amazon VPC nella Guida per l'utente di Amazon Virtual Private Cloud.

   b. (Facoltativo) Per Subnet, scegli la sottorete in cui vuoi lanciare l'istanza Amazon EC2 .

   c. Per Assegna automaticamente IP pubblico, scegli Abilita.

7. Nella sottosezione Firewall (gruppi di sicurezza), rivedi le impostazioni preconfigurate. Se lo desideri, puoi modificare il nome e la descrizione predefiniti del nuovo gruppo di sicurezza da creare per la tua EC2 istanza Amazon, oppure scegliere di applicare le regole firewall di un gruppo di sicurezza esistente.
8. Nella sottosezione Regole dei gruppi di sicurezza in ingresso, aggiungi le regole firewall per aprire le porte che i client utilizzeranno per connettersi alla tua istanza. Per ulteriori informazioni sulle porte richieste per Amazon S3 File Gateway Amazon FSx File , consulta Requisiti delle porte Requisiti delle . Per ulteriori informazioni sull'aggiunta di regole firewall, consulta Regole del gruppo di sicurezza nella Guida per l'utente di Amazon Elastic Compute Cloud per le istanze Linux.

> **Note**
>
> Amazon S3 File Gateway richiede che la porta TCP 80 sia aperta per il traffico in entrata e l'accesso HTTP una tantum durante l'attivazione del gateway. Dopo l'attivazione, è possibile chiudere questa porta.
> Se prevedi di creare condivisioni di file NFS, devi aprire la TCP/UDP porta 2049 per l'accesso NFS, la porta 111 per l'accesso e la TCP/UDP porta 20048 per NFSv3 l'accesso. TCP/UDP NFSv3
> Se si prevede di creare condivisioni di file SMB, è necessario aprire la porta TCP 445 per l'accesso SMB.

9. Nella sottosezione Configurazione di rete avanzata, rivedere le impostazioni preconfigurate e, se necessario, apportare modifiche.
10. Nella sezione Configura archiviazione scegliere Aggiungi nuovo volume per aggiungere spazio di archiviazione all'istanza del gateway.

> **Important**
>
> È necessario aggiungere almeno un volume Amazon EBS con almeno 150 GiB di capacità per lo storage della cache oltre al volume root preconfigurato. Per migliorare le prestazioni, consigliamo di allocare più volumi EBS per lo storage della cache con almeno 150 GiB ciascuno.

11. Nella sezione Dettagli avanzati, rivedi le impostazioni preconfigurate e apporta le modifiche se necessario.

12. Scegli Launch instance per avviare la tua nuova istanza Amazon EC2 gateway con le impostazioni configurate.
13. Per verificare che la tua nuova istanza sia stata lanciata correttamente, vai alla pagina Istanze nella EC2 console Amazon e cerca la tua nuova istanza per nome. Assicurati che in Stato dell'istanza sia visualizzato In esecuzione con un segno di spunta verde e che il Controllo dello stato sia completo e mostri un segno di spunta verde.
14. Seleziona l'istanza dalla pagina dei dettagli.

È possibile determinare l'ID AMI da utilizzare per avviare un File Gateway utilizzando la console Storage Gateway o interrogando l'archivio AWS Systems Manager dei parametri.

Per determinare l'ID AMI, procedi in uno dei seguenti modi:

- Inizia la configurazione di un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, consulta Configurare un Amazon S3 File Gateway Gateway. Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come piattaforma host, quindi scegli Launch instance per aprire il modello Gateway di archiviazione AWS AMI nella EC2 console Amazon.

  Verrai reindirizzato alla pagina AMI della EC2 community, dove puoi vedere l'ID AMI per la tua AWS regione nell'URL.
- Esegui una query sull'archivio dei parametri Systems Manager. È possibile utilizzare l'API AWS CLI o Storage Gateway per interrogare il parametro pubblico Systems Manager nello spazio dei nomi `/aws/service/storagegateway/ami/FILE_S3/latest`. Ad esempio, l'utilizzo del seguente comando CLI restituisce l'ID dell'AMI corrente nel campo Regione AWS specificato.

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  FILE_S3/latest
  ```

  Il comando CLI restituisce un output simile al seguente:

  ```
  {
      "Parameter": {
          "Type": "String",
          "LastModifiedDate": 1561054105.083,
          "Version": 4,
          "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
  FILE_S3/latest",
          "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
  ```

```
        "Value": "ami-123c45dd67d891000"
    }
}
```

Modifica le opzioni dei metadati delle EC2 istanze Amazon

Il servizio di metadati dell'istanza (IMDS) è un componente su istanza che fornisce un accesso sicuro ai metadati delle istanze Amazon EC2 . Un'istanza può essere configurata per accettare richieste di metadati in entrata che utilizzano IMDS versione 1 (IMDSv1) o richiedere che tutte le richieste di metadati utilizzino IMDS versione 2 (). IMDSv2 IMDSv2 utilizza richieste orientate alla sessione e mitiga diversi tipi di vulnerabilità che potrebbero essere utilizzate per tentare di accedere all'IMDS. Per informazioni su IMDSv2, consulta Come funziona Instance Metadata Service versione 2 nella Amazon Elastic Compute Cloud User Guide.

Ti consigliamo di richiederlo IMDSv2 per tutte le EC2 istanze Amazon che ospitano Storage Gateway. IMDSv2 è obbligatorio per impostazione predefinita su tutte le istanze gateway appena lanciate. Se disponi di istanze esistenti che sono ancora configurate per accettare richieste di IMDSv1 metadati, consulta Require the use of IMDSv2 nella Amazon Elastic Compute Cloud User Guide per istruzioni su come modificare le opzioni di metadati dell'istanza di cui richiedere l'uso. IMDSv2 L'applicazione di questa modifica non richiede il riavvio dell'istanza.

Sincronizza l'ora della macchina virtuale con l'ora dell'host KVM Hyper-V o Linux

Per un gateway distribuito su VMware ESXi, l'impostazione dell'ora dell'host dell'hypervisor e la sincronizzazione dell'ora della macchina virtuale con l'host sono sufficienti per evitare variazioni di orario. Per ulteriori informazioni, consulta Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware . Per un gateway distribuito su Microsoft Hyper-V o Linux KVM, si consiglia di controllare periodicamente l'ora della macchina virtuale utilizzando la procedura descritta di seguito.

Per visualizzare e sincronizzare l'ora di una macchina virtuale gateway hypervisor con un server Network Time Protocol (NTP)

1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.

- Per ulteriori informazioni sull'accesso alla console locale per una macchina virtuale basata su kernel Linux (KVM), vedere. Accesso alla console locale del gateway con Linux KVM

2. Nella schermata del menu principale di Storage Gateway Configuration, immettere il numero corrispondente per selezionare System Time Management.
3. Nella schermata del menu System Time Management, immettere il numero corrispondente per selezionare Visualizza e sincronizza l'ora del sistema.

   La console locale del gateway visualizza l'ora corrente del sistema e la confronta con l'ora riportata dal server NTP, quindi riporta l'esatta discrepanza tra i due orari in secondi.
4. Se la discrepanza temporale è superiore a 60 secondi, immettere **y** per sincronizzare l'ora del sistema con l'ora NTP. In caso contrario, inserire **n**.

   La sincronizzazione dell'ora potrebbe richiedere alcuni minuti.

Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware

Per attivare il gateway, devi assicurarti che la data e l'ora della macchina virtuale siano sincronizzate con quelle dell'host e che queste siano impostate correttamente. In questa sezione devi prima sincronizzare la data e l'ora nella macchina virtuale con quelle dell'host. Devi quindi controllare la data e l'ora dell'host e, se necessario, impostarle e configurare l'host per la sincronizzazione automatica con un server NTP (Network Time Protocol).

> **Important**
>
> La sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host è necessaria per una corretta attivazione del gateway.

Per sincronizzare la data e l'ora della macchina virtuale con quelle dell'host

1. Configurare la data e l'ora della macchina virtuale.

   a. Nel client vSphere, fare clic con il pulsante destro del mouse sul nome della macchina virtuale gateway nel pannello sul lato sinistro della finestra dell'applicazione per aprire il menu contestuale della macchina virtuale, quindi scegliere Modifica impostazioni.

      Viene visualizzata la finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale).

b. Scegli la scheda Opzioni, quindi scegli VMware Strumenti dall'elenco delle opzioni.

c. Seleziona l'opzione Sincronizza l'ora dell'ospite con l'host nella sezione Avanzate sul lato destro della finestra di dialogo Proprietà della macchina virtuale, quindi scegli OK.

   La macchina virtuale sincronizza le proprie data e ora con quelle dell'host.

2. Configurare la data e l'ora dell'host.

   È importante verificare che l'orologio dell'host sia impostato sulla data e sull'ora corrette. Se non hai configurato l'orologio dell'host, completa la procedura seguente per impostarlo e sincronizzarlo con un server NTP.

   a. Nel client VMware vSphere, selezionare il nodo host vSphere nel pannello a sinistra, quindi scegliere la scheda Configurazione.

   b. Selezionare Time Configuration (Configurazione data e ora) nel pannello Software e quindi scegliere il collegamento Properties (Proprietà).

      Viene visualizzata la finestra di dialogo Time Configuration (Configurazione data e ora).

   c. In Data e ora, impostare la data e l'ora per l'host vSphere.

   d. Configurare l'host per la sincronizzazione automatica di data e ora con un server NTP.

      i. Scegli Opzioni nella finestra di dialogo Time Configuration, quindi nella finestra di dialogo Opzioni NTP Daemon (ntpd), scegli Impostazioni NTP nel pannello di sinistra.

      ii. Scegliere Add (Aggiungi) per aggiungere un nuovo server NTP.

      iii. Nella finestra di dialogo Add NTP Server (Aggiungi server NTP) digitare l'indirizzo IP o il nome di dominio completo di un server NTP e quindi scegliere OK.

         È possibile utilizzare `pool.ntp.org` come nome di dominio.

      iv. Nella finestra di dialogo Opzioni del demone NTP (ntpd), scegli Generale nel pannello di sinistra.

      v. In Comandi di servizio, scegliete Avvia per avviare il servizio.

         Se si modifica questo riferimento al server NTP o successivamente si aggiunge un altro server, sarà necessario riavviare il servizio per usare il nuovo server.

   e. Scegliere OK per chiudere la finestra di dialogo NTP Daemon (ntpd) Options (Opzioni daemon NTP - ntpd).

f. Scegliere OK per chiudere la finestra di dialogo Time Configuration (Configurazione data e ora).

Configurazione degli adattatori di rete per il gateway

Storage Gateway utilizza un singolo adattatore di rete VMXNET3 (10 GbE) per impostazione predefinita, ma è possibile configurare il gateway in modo che utilizzi più di un adattatore di rete in modo che sia accessibile da più indirizzi IP. Tale condizione torna utile nei seguenti casi:

- Massimizzazione del throughput: è possibile massimizzare la velocità di trasmissione verso un gateway quando gli adattatori di rete rappresentano un collo di bottiglia.
- Separazione delle applicazioni: potrebbe essere necessario distinguere le modalità di scrittura delle applicazioni sui volumi di un gateway. Potresti, ad esempio, scegliere di far utilizzare a un'applicazione critica di storage una scheda apposita per il tuo gateway.
- Vincoli di rete: l'ambiente applicativo potrebbe richiedere di mantenere le condivisioni di file e gli iniziatori che si connettono ad esse in una rete isolata. Tale rete è diversa da quella con cui il gateway comunica con AWS.

In un tipico caso di utilizzo con più adattatori, un adattatore è configurato come route con cui il gateway comunica AWS (ovvero come gateway predefinito). Ad eccezione di questo adattatore, gli iniziatori devono trovarsi nella stessa sottorete dell'adattatore che contiene le condivisioni di file a cui si connettono. per non compromettere la comunicazione con le destinazioni programmate. Se una destinazione è configurata sullo stesso adattatore con cui viene utilizzata la comunicazione AWS, il traffico di condivisione di file per quella destinazione e il AWS traffico fluiscono attraverso lo stesso adattatore.

In alcuni casi, è possibile configurare un adattatore per la connessione alla console Storage Gateway e quindi aggiungere un secondo adattatore. In tal caso, Storage Gateway configura automaticamente la tabella di routing per utilizzare il secondo adattatore come route preferita. Per istruzioni su come configurare più adattatori, vedere i seguenti argomenti:

Argomenti

- Configurazione del gateway per più utenti NICs su un host VMware ESXi
- Configurazione del gateway per più utenti NICs in Microsoft Hyper-V Host

Configurazione del gateway per più utenti NICs su un host VMware ESXi

La procedura seguente presuppone che la macchina virtuale gateway disponga già di una scheda di rete definita e descrive come aggiungerne una. VMware ESXi

Per configurare il gateway per l'utilizzo di un adattatore di rete aggiuntivo nell'host VMware ESXi

1. Arresta il gateway.
2. Nel client VMware vSphere, selezionare la macchina virtuale gateway.

   Per questa procedura, la macchina virtuale può rimanere attiva.
3. Nel client, apri il menu contestuale (clic con il pulsante destro del mouse) per la VM del gateway e scegli Edit Settings (Modifica impostazioni).
4. Nella scheda Hardware della finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale), scegli Add (Aggiungi) per aggiungere un dispositivo.
5. Segui la procedura guidata Add Hardware (Aggiungi hardware) per aggiungere una scheda di rete.

   a. Nel riquadro Device Type (Tipo di dispositivo), scegli Ethernet Adapter (Scheda Ethernet) per aggiungere una scheda, quindi scegli Next (Avanti).
   b. Nel riquadro Network Type (Tipo di rete), assicurati che Connect at power on (Connetti all'accensione) sia selezionato per Type (Tipo), quindi scegli Next (Avanti).

      Si consiglia di utilizzare l'adattatore di VMXNET3 rete con Storage Gateway. Per ulteriori informazioni sui tipi di adattatore che potrebbero apparire nell'elenco degli adattatori, vedere Tipi di adattatori di rete nella ESXi documentazione di vCenter Server.
   c. Nel riquadro Ready to Complete (Pronto al completamento), rivedi le informazioni, quindi scegli Finish (Fine).
6. Scegli la scheda Riepilogo della VM, quindi scegli Visualizza tutto accanto alla casella Indirizzo IP. Nella finestra Indirizzi IP macchina virtuale vengono visualizzati tutti gli indirizzi IP da poter utilizzare per accedere al gateway. Verifica che un secondo indirizzo IP sia elencato per il gateway.

> **Note**
>
> Potrebbero volerci alcuni istanti prima che le modifiche della scheda diventino effettive e che le informazioni di riepilogo della VM si aggiornino.

7. Nella console Storage Gateway, accendere il gateway.
8. Nel riquadro Navigazione della console Storage Gateway, scegliere Gateway, quindi scegliere il gateway a cui aggiungere la scheda. Verificare che il secondo indirizzo IP sia presente nell'elenco nella scheda Details (Dettagli).

> **Note**
>
> I comandi di montaggio di esempio forniti nella pagina delle informazioni per una condivisione di file nella console Storage Gateway includeranno sempre l'indirizzo IP dell'adattatore di rete che è stato aggiunto più di recente al gateway associato alla condivisione di file.

Per informazioni sulle attività della console locale comuni agli VMware host Hyper-V e KVM, vedere Esecuzione di attività sulla console locale della macchina virtuale

Configurazione del gateway per più utenti NICs in Microsoft Hyper-V Host

La procedura seguente presuppone che la macchina virtuale del gateway disponga già di una scheda di rete definita e che si aggiunga una seconda scheda. Questa procedura mostra come aggiungere una scheda per un host Microsoft Hyper-V.

Per configurare il gateway per l'uso di una scheda di rete aggiuntiva in un host Microsoft Hyper-V

1. Nella console Storage Gateway, spegnere il gateway.
2. In Microsoft Hyper-V Manager, seleziona la tua macchina virtuale gateway dal pannello Macchine virtuali.
3. Se la macchina virtuale gateway non è già disattivata, fai clic con il pulsante destro del mouse sul nome della macchina virtuale per aprire il menu contestuale, quindi scegli Disattiva.
4. Fai clic con il pulsante destro del mouse sul nome della macchina virtuale del gateway per aprire il menu contestuale, quindi scegli Impostazioni.
5. Nella finestra di dialogo Impostazioni, in Hardware, scegli Aggiungi hardware.
6. Nel pannello Aggiungi hardware sul lato destro della finestra di dialogo Impostazioni, scegli Adattatore di rete, quindi scegli Aggiungi per aggiungere un dispositivo.
7. Configurare la scheda di rete e quindi scegliere Apply (Applica) per applicare le impostazioni.
8. Nella finestra di dialogo Impostazioni, in Hardware, confermate che la nuova scheda di rete è stata aggiunta all'elenco hardware, quindi scegliete OK.

9. Accendere il gateway utilizzando la console Storage Gateway.
10. Nel pannello di navigazione della console Storage Gateway, scegli Gateway, quindi seleziona il gateway a cui hai aggiunto l'adattatore. Verifica che un secondo indirizzo IP sia elencato nella scheda Dettagli.

> **Note**
>
> I comandi di montaggio di esempio forniti nella pagina delle informazioni per una condivisione di file nella console Storage Gateway includeranno sempre l'indirizzo IP dell'adattatore di rete che è stato aggiunto più di recente al gateway associato alla condivisione di file.

Per informazioni sulle attività della console locale comuni agli host VMware Hyper-V e KVM, vedere Esecuzione di attività sulla console locale della macchina virtuale

Utilizzo di VMware vSphere High Availability con Storage Gateway

Storage Gateway offre un'elevata disponibilità VMware tramite una serie di controlli di integrità a livello di applicazione integrati con VMware vSphere High Availability (HA). VMware Questo approccio consente di proteggere i carichi di lavoro di storage da errori di hardware, hypervisor o rete. Consente inoltre di proteggere da errori di software, come il timeout di connessione e condivisione file o l'indisponibilità del volume.

Con questa integrazione, un gateway distribuito in un VMware ambiente locale o in un VMware cloud on si ripristina AWS automaticamente dalla maggior parte delle interruzioni del servizio. Generalmente il processo dura meno di 60 secondi senza perdita di dati.

> **Note**
>
> Si consiglia di effettuare le seguenti operazioni se si implementa Storage Gateway in un cluster VMware HA:
>
> - Implementare il pacchetto scaricabile VMware ESX .ova che contiene la macchina virtuale Storage Gateway su un solo host in un cluster.
> - Quando si distribuisce il pacchetto .ova, selezionare un data store che non sia locale su un host. Al contrario, utilizzare un datastore accessibile a tutti gli host del cluster. Se si seleziona un datastore locale per un host e l'host ha esito negativo, l'origine dati potrebbe

non essere accessibile ad altri host del cluster e il failover su un altro host potrebbe non riuscire.

- Con il clustering, se distribuisci il pacchetto .ova nel cluster, seleziona un host quando ti viene richiesto di farlo. In alternativa, puoi distribuire direttamente a un host in un cluster.

I seguenti argomenti descrivono come implementare Storage Gateway in un cluster VMware HA:

Argomenti

- Configurazione del cluster vSphere VMware HA
- Configura il tipo di gateway
- Distribuzione del gateway
- (Facoltativo) Aggiungi opzioni Override for Other VMs sul tuo cluster
- Attivazione del gateway
- Testa la tua configurazione VMware ad alta disponibilità

Configurazione del cluster vSphere VMware HA

Innanzitutto, se non hai già creato un VMware cluster, creane uno. Per informazioni su come creare un VMware cluster, vedere Create a vSphere HA Cluster nella VMware documentazione.

Successivamente, configura il VMware cluster in modo che funzioni con Storage Gateway.

Per configurare il VMware cluster

1. Nella pagina Modifica impostazioni cluster in VMware vSphere, assicurarsi che il monitoraggio delle macchine virtuali sia configurato per il monitoraggio delle macchine virtuali e delle applicazioni. A tale scopo, imposta i seguenti valori per ciascuna opzione:

   - Risposta all'errore dell'host: riavvio VMs
   - Risposta per l'isolamento dell'host: spegnimento e riavvio VMs
   - Datastore with PDL (Datastore con PDL): Disabled (Disabilitato)
   - Datastore with APD (Datastore con APD): Disabled (Disabilitato)
   - VM Monitoring (Monitoraggio VM) : VM and Application Monitoring (Monitoraggio VM e applicazioni)
2. Ottimizzare la sensibilità del cluster regolando i seguenti valori:

- Intervallo di errore: dopo questo intervallo, la macchina virtuale viene riavviata se non viene ricevuto un heartbeat VM.
- Tempo di attività minimo: tempo di attesa del cluster dopo che una macchina virtuale inizia a monitorare gli heartbeat degli strumenti VM.
- Numero massimo di reimpostazioni per VM: il cluster riavvia la macchina virtuale per un numero massimo di volte all'interno della finestra temporale massima di ripristino.
- Finestra temporale massima reimpostazioni: la finestra temporale entro cui contare il numero massimo di reimpostazioni per VM.

Se non si è sicuri di quali valori impostare, utilizzare queste impostazioni di esempio:

- Failure interval (Intervallo di errore): **30** secondi
- Minimum uptime (Tempo di attività minimo): **120** secondi
- Maximum per-VM resets (Numero massimo reimpostazioni VM): **3**
- Maximum resets time window (Finestra temporale massima reimpostazioni): **1** ora

Se ne hai altri VMs in esecuzione sul cluster, potresti voler impostare questi valori in modo specifico per la tua macchina virtuale. Non è possibile eseguire questa operazione fino a quando non distribuisci la VM dal file .ova. Per ulteriori informazioni sull'impostazione di questi valori, consulta (Facoltativo) Aggiungi opzioni Override for Other VMs sul tuo cluster.

Configura il tipo di gateway

Utilizzare la seguente procedura per configurare il gateway

Per scaricare l'immagine .ova per il tipo di gateway

- Scarica l'immagine .ova per il tipo di gateway di una delle seguenti opzioni:
  - File Gateway — Crea e attiva un Amazon S3 File Gateway

Distribuzione del gateway

Nel cluster configurato distribuisci l'immagine .ova in uno degli host del cluster. Per istruzioni, vedere Distribuire un modello OVF o OVA nella documentazione online di VMware vSphere.

Per distribuire l'immagine .ova del gateway

1. Distribuire l'immagine .ova in uno degli host del cluster.
2. Assicurarsi che i datastore scelti per il disco root e la cache siano disponibili per tutti gli host del cluster.

(Facoltativo) Aggiungi opzioni Override for Other VMs sul tuo cluster

Se ne hai altri VMs in esecuzione sul tuo cluster, potresti voler impostare i valori del cluster in modo specifico per ogni macchina virtuale. Per istruzioni, vedere Personalizzazione di una singola macchina virtuale nella documentazione online di VMware vSphere.

Per aggiungere opzioni di override per altre VMs nel tuo cluster

1. Nella pagina Riepilogo di VMware vSphere, scegliere il cluster per aprire la pagina del cluster, quindi scegliere Configura.
2. Scegliere la scheda Configuration (Configurazione) e quindi scegliere VM Overrides (Sostituzioni VM).
3. Aggiungere una nuova opzione di sostituzione VM per modificare ogni valore.

   Impostare i seguenti valori per ciascuna opzione in vSphere HA - VM Monitoring:

   - Monitoraggio VM: Override Enabled - Monitoraggio di macchine virtuali e applicazioni
   - Sensibilità di monitoraggio delle macchine virtuali: Override Enabled - Monitoraggio di macchine virtuali e applicazioni
   - Monitoraggio delle VM: personalizzato
   - Intervallo di errore: secondi **30**
   - Tempo di attività minimo: secondi **120**
   - Maximum per-VM resets (Numero massimo reimpostazioni VM): **5**
   - Intervallo di tempo massimo di ripristino: entro ore **1**

Attivazione del gateway

Dopo aver implementato il file.ova nell' VMware ambiente, attiva il gateway utilizzando la console Storage Gateway. Per istruzioni, consulta Rivedi le impostazioni e attiva Amazon S3 File Gateway Gateway.

Testa la tua configurazione VMware ad alta disponibilità

Dopo aver attivato il gateway, esegui il test della configurazione.

Per testare la tua configurazione VMware HA

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway che desideri testare per VMware HA.
3. Per Azioni, scegli Verifica VMware HA.
4. Nella casella Verify VMware High Availability Configuration che appare, scegli OK.

   > **Note**
   >
   > Il test della configurazione VMware HA riavvia la macchina virtuale del gateway e interrompe la connettività al gateway. L'esecuzione del test potrebbe richiedere alcuni minuti.

   Se il test ha esito positivo, lo stato Verified (Verificato) viene visualizzato nella scheda dettagli del gateway nella console.
5. Scegliere Exit (Esci).

Puoi trovare informazioni sugli eventi VMware HA nei gruppi di CloudWatch log di Amazon. Per ulteriori informazioni, consulta Ottenere i registri di integrità di S3 FSx File Gateway con CloudWatch gruppi di log.

Ottenimento di una chiave di attivazione per il gateway

Per ricevere una chiave di attivazione per il gateway, effettua una richiesta Web alla macchina virtuale (VM) del gateway. La macchina virtuale restituisce un reindirizzamento che contiene la chiave di attivazione, che viene passata come uno dei parametri dell'opzione `ActivateGateway` API per specificare la configurazione del gateway. Per ulteriori informazioni, vedere ActivateGatewaylo Storage Gateway API Reference.

> **Note**
>
> Le chiavi di attivazione del gateway scadono dopo 30 minuti se non vengono utilizzate.

La richiesta effettuata alla macchina virtuale gateway include la AWS regione in cui avviene l'attivazione. L'URL restituito dal reindirizzamento nella risposta contiene un parametro della stringa di query denominato `activationkey`. Questo parametro della stringa di query è la chiave di attivazione. Il formato della stringa di query ha un aspetto simile a questo: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. L'output di questa query restituisce sia la regione che la chiave di attivazione.

L'URL include anche `vpcEndpoint`, l'ID dell'endpoint VPC per i gateway che si connettono utilizzando il tipo di endpoint VPC.

> **Note**
>
> L'appliance hardware AWS Storage Gateway, i modelli di immagini VM e Amazon EC2 Amazon Machine Images (AMI) sono preconfigurati con i servizi HTTP necessari per ricevere e rispondere alle richieste Web descritte in questa pagina. Non è richiesta né consigliata l'installazione di servizi aggiuntivi sul gateway.

Argomenti

- Linux (curl)
- Linux (bash/zsh)
- Microsoft Windows PowerShell
- Utilizzo della console locale

Linux (curl)

Gli esempi seguenti mostrano come recuperare una chiave di attivazione utilizzando Linux (curl).

> **Note**
>
> Sostituisci le variabili evidenziate con i valori effettivi per il gateway. I valori accettabili sono i seguenti:

- *gateway_ip_address*- L' IPv4 indirizzo del gateway, ad esempio `172.31.29.201`
- *gateway_type*- Il tipo di gateway che desideri attivare, ad esempio `STOREDCACHED`,`VTL`,`FILE_S3`, o`FILE_FSX_SMB`.
- *region_code*- La regione in cui desideri attivare il gateway. Consulta Endpoint regionali nella Guida di riferimento generale.AWS Se questo parametro non è specificato o se il valore fornito è digitato in modo errato o non corrisponde a una regione valida, il comando utilizzerà per impostazione predefinita la `us-east-1` regione.
- *vpc_endpoint*- Il nome dell'endpoint VPC per il gateway, ad esempio. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Endpoint pubblico

Per ottenere una chiave di attivazione per un endpoint pubblico, usa uno dei seguenti comandi:

Endpoint standard

Per ottenere la chiave di attivazione per un endpoint standard:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Endpoint dual-stack

Per ottenere la chiave di attivazione per un endpoint dual-stack:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

Endpoint FIPS

Per ottenere la chiave di attivazione per un endpoint FIPS:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

Endpoint VPC

Per ottenere la chiave di attivazione per un endpoint VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

L'esempio seguente mostra come usare Linux (bash/zsh) per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

L'esempio seguente mostra come utilizzare Microsoft Windows PowerShell per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Utilizzo della console locale

Gli esempi seguenti mostrano

Gateway basati su Amazon Linux 2 (AL2)

È possibile selezionare endpoint standard o FIPS per i gateway basati su. AL2

> **Note**
>
> Gli endpoint FIPS non sono disponibili in tutti. Regioni AWS Per ulteriori informazioni, vedere FIPS Endpoints by Service.

Per ottenere una chiave di attivazione per il gateway AL2 basato sulla console locale

1. Accedi alla tua console locale come amministratore.

2. Dal menu principale Attivazione dell'AWS appliance - Configurazione, seleziona `0` Ottieni chiave di attivazione.
3. Seleziona Storage Gateway come opzione di famiglia di gateway.
4. Inserisci la AWS regione in cui desideri attivare il gateway.
5. Per il tipo di rete, inserisci 1 Public o 2 VPC.
6. Per il tipo di endpoint, inserisci 1 Standard o 2 Federal Information Processing Standard (FIPS).

Gateway basati su Amazon Linux 2023 (AL2023)

Per i gateway basati su AL2 023, sono disponibili i seguenti endpoint:

- Endpoint standard (solo supporto) IPv4
- Endpoint FIPS (solo supporto) IPv4
- Endpoint dual-stack (supporto e) IPv4 IPv6
- Endpoint FIPS dual-stack (supporto e) IPv4 IPv6

Per ulteriori informazioni, consulta Tipi di endpoint.

Per ottenere una chiave di attivazione per il gateway basato su AL2 023 dalla console locale

1. Accedere alla tua console locale. Se ti connetti alla tua EC2 istanza Amazon da un computer Windows, accedi come amministratore.
2. Dal menu principale Attivazione dell'AWS appliance - Configurazione, seleziona `0` Ottieni chiave di attivazione.
3. Seleziona Storage Gateway come opzione di famiglia di gateway.
4. Inserisci la AWS regione in cui desideri attivare il gateway.
5. Per il tipo di rete, inserisci 1 Public o 2 per endpoint VPC.
6. Per Seleziona il tipo di endpoint, Abilita FIPS? , immettere `Y` per abilitare FIPS o per utilizzare un endpoint `N` non FIPS.
7. Per il tipo di endpoint, inserisci per endpoint standard o 1 per endpoint dual-stack. 2
    - Per un endpoint dual-stack, per Seleziona la versione IP o exit:, inserisci for o for. 1 IPv4 2 IPv6

Support per gli attributi dei file in Amazon S3 File Gateway

Amazon S3 File Gateway supporta gli attributi di file DOS o Windows per impostazione predefinita. Utilizzando S3 File Gateway, puoi conservare i dati e i metadati dei file e aggiornare le impostazioni, ad esempio contrassegnare gli articoli come archiviati quando vengono inseriti in Amazon S3. Per ulteriori informazioni sugli attributi dei file DOS e Windows, consulta l'articolo File Attribute Constants sul sito Web dedicato alla documentazione sullo sviluppo di app Windows.

S3 File Gateway supporta i seguenti attributi:

- ReadOnly— S3 File Gateway impedisce le modifiche ai file con l' ReadOnly attributo impostato.
- Archivio: S3 File Gateway imposta questo attributo quando i file vengono aggiunti per la prima volta al gateway.

> **Note**
>
> Le applicazioni di backup in genere eseguono il backup dei file con il bit di archiviazione impostato e quindi cancellano il bit dopo il successo del backup.

- Nascosto: i client Server Message Block (SMB) nascondono i file che utilizzano questo set di bit.
- Sistema: questo attributo persiste dopo averlo impostato.

Quando copi un file su S3 File Gateway con gli attributi impostati, gli attributi DOS o Windows del file vengono conservati su S3 File Gateway e in Amazon S3. Puoi aggiornare questi attributi per i file sul gateway e tali aggiornamenti si applicano anche all'oggetto in Amazon S3. Se un file viene rimosso dal gateway, il gateway estrae il file, i relativi metadati e gli attributi persistenti da Amazon S3 quando lo richiedi.

> **Note**
>
> Gli attributi DOS sono supportati solo sulle condivisioni SMB e se l'accesso è controllato dagli elenchi di controllo degli accessi di Windows.

Utilizzo Direct Connect con Storage Gateway

Direct Connect collega la tua rete interna ad Amazon Web Services Cloud. Utilizzando Direct Connect Storage Gateway, è possibile creare una connessione per esigenze di carichi di lavoro ad alta velocità, fornendo una connessione di rete dedicata tra il gateway locale e. AWS

Storage Gateway utilizza endpoint pubblici. Una volta Direct Connect stabilita una connessione, è possibile creare un'interfaccia virtuale pubblica per consentire l'instradamento del traffico verso gli endpoint Storage Gateway. L'interfaccia virtuale pubblica ignora i provider di servizi Internet nel percorso di rete. L'endpoint pubblico del servizio Storage Gateway può trovarsi nella stessa AWS regione della Direct Connect posizione o in una AWS regione diversa.

La figura seguente mostra un esempio di come Direct Connect funziona con Storage Gateway. architettura di rete che mostra Storage Gateway connesso al cloud tramite connessione AWS diretta.

La procedura seguente presuppone che è stato creato un funzionamento gateway.

Da utilizzare Direct Connect con Storage Gateway

1. Crea e stabilisci una AWS Direct Connect connessione tra il data center locale e l'endpoint Storage Gateway. Per ulteriori informazioni su come creare una connessione, consulta Nozioni di base su Direct Connect nella Guida per l'utente di Direct Connect .
2. Connect l'appliance Storage Gateway locale al Direct Connect router.
3. Creare un'interfaccia virtuale pubblica e configurare il router locale di conseguenza. Per ulteriori informazioni, consulta Creazione di un'interfaccia virtuale nella Guida per l'utente di Direct Connect .

Per ulteriori informazioni Direct Connect, consulta What is? Direct Connect nella Guida Direct Connect per l'utente.

Requisiti di autorizzazione degli account del servizio Active Directory

Se prevedi di utilizzare Microsoft Active Directory per fornire l'accesso autenticato all'utente ai file system delle condivisioni sul tuo Gateway di archiviazione AWS, devi assicurarti di disporre di un account del servizio Active Directory e che l'account del servizio disponga delle autorizzazioni delegate per aggiungere computer al tuo dominio. Un account di servizio è un account utente di

Active Directory a cui è stata delegata l'autorizzazione per eseguire determinate attività. Fornisci le credenziali di nome utente e password per questo account quando ti colleghi a uno Storage Gateway al tuo dominio Active Directory.

All'account del servizio Active Directory devono essere delegate le seguenti autorizzazioni nell'unità organizzativa a cui si accede al gateway:

- Capacità di creare ed eliminare oggetti informatici
- Possibilità di reimpostare le password
- Possibilità di modificare le autorizzazioni
- Possibilità di impedire agli account di leggere e scrivere dati
- Capacità convalidata di leggere e scrivere le restrizioni relative all'account
- Capacità convalidata di scrivere sul nome principale del servizio
- Capacità convalidata di scrivere sul nome host DNS

Queste rappresentano il set minimo di autorizzazioni necessarie per unire gli oggetti del computer ad Active Directory. Per ulteriori informazioni, vedere l'argomento della documentazione di Microsoft Windows Server Errore: accesso negato quando utenti non amministratori a cui è stato delegato il controllo tentano di aggiungere computer a un controller di dominio.

Ottenere l'indirizzo IP per il dispositivo gateway

Dopo aver scelto un host e distribuito la macchina virtuale gateway, è possibile connettere e attivare il gateway. Per eseguire questa operazione, è necessario l'indirizzo IP della macchina virtuale gateway. L'indirizzo IP si ottiene dalla console locale del gateway. È possibile effettuare l'accesso alla console locale e ottenere l'indirizzo IP nella parte superiore della pagina della console.

Per i gateway distribuiti in locale, è anche possibile ottenere l'indirizzo IP dall'hypervisor. Per i EC2 gateway Amazon, puoi anche ottenere l'indirizzo IP della tua EC2 istanza Amazon dalla Console di EC2 gestione Amazon. Per informazioni su come ottenere l'indirizzo IP del gateway, consulta:

- VMware ospitante: Accesso alla console locale del gateway con VMware ESXi
- Host HyperV: Accesso alla console locale del gateway con Microsoft Hyper-V
- Host di macchina virtuale basata su kernel (KVM) Linux: Accesso alla console locale del gateway con Linux KVM

- EC2 ospitante: Ottenere un indirizzo IP da un EC2 host Amazon

Quando individui l'indirizzo IP, annotalo. Quindi torna alla console Storage Gateway e digita l'indirizzo IP nella console.

Ottenere un indirizzo IP da un EC2 host Amazon

Per ottenere l'indirizzo IP dell' EC2 istanza Amazon su cui è distribuito il gateway, accedi alla console locale dell' EC2 istanza. Quindi ottenere l'indirizzo IP nella parte superiore della pagina della console. Per istruzioni, consulta .

Puoi anche ottenere l'indirizzo IP dalla Console di EC2 gestione Amazon. Consigliamo di usare l'indirizzo IP pubblico per l'attivazione. Per ottenere l'indirizzo IP pubblico, utilizzare la procedura 1. Se si sceglie invece di utilizzare l'indirizzo IP elastico, consulta la procedura 2.

Procedura 1: per connettersi al gateway utilizzando l'indirizzo IP pubblico

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, quindi seleziona l' EC2 istanza su cui è distribuito il gateway.
3. Scegliere la scheda Description (Descrizione) in basso, quindi annotare l'indirizzo IP pubblico. Utilizzarlo per collegarsi al gateway. Tornare alla console Storage Gateway e digitare l'indirizzo IP.

Per utilizzare l'indirizzo IP elastico per l'attivazione, procedere nel modo seguente.

Procedura 2: per connettersi al gateway utilizzando l'indirizzo IP elastico

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, quindi seleziona l' EC2 istanza su cui è distribuito il gateway.
3. Scegliere la scheda Description (Descrizione) in basso, quindi annotare il valore Elastic IP (IP elastico). Utilizzarlo per collegarsi al gateway. Tornare alla console Storage Gateway e digitare l'indirizzo IP elastico.

IPv6 supporto

IPv6 il supporto è disponibile solo per le versioni 2.x o successive delle appliance gateway. L'appliance Gateway versione 1.x non può essere aggiornata alla versione 2.x. È necessario migrare o sostituire la versione 1.x del dispositivo gateway per ottenere assistenza. IPv6

I seguenti endpoint dual-stack sono necessari per. IPv6

```
storagegateway.region.api.aws:443
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
s3.dualstack.region.amazonaws.com
```

Informazioni sulle risorse e sulle risorse di Storage Gateway IDs

In Storage Gateway, la risorsa principale è un gateway, ma altri tipi di risorse è la condivisione di file. Le condivisioni di file vengono chiamate sottorisorse e non esistono a meno che non siano associate a un gateway.

A queste risorse e sottorisorse sono associati Amazon Resource Names (ARNs) univoci, come mostrato in questa tabella.

Tipo di risorsa	Formato ARN
ARN gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN condivisione file	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

Lavorare con Resource IDs

Quando crei una risorsa, Storage Gateway assegna a tale risorsa un ID risorsa univoco. Questo ID risorsa è parte dell'ARN della risorsa. Un ID risorsa ha il formato di un identificatore di risorsa seguito

da un trattino e da una combinazione univoca di otto lettere e numeri. Ad esempio, un ID gateway ID ha il formato `sgw-12A3456B` dove `sgw` è l'identificativo della risorsa per i gateway.

IDs Le risorse Storage Gateway sono in lettere maiuscole. Tuttavia, quando utilizzi queste risorse IDs con l' EC2 API Amazon, Amazon EC2 si aspetta che la risorsa sia IDs in lettere minuscole. È necessario modificare l'ID della risorsa in minuscolo per utilizzarlo con l'API. EC2 Ad esempio, in Storage Gateway l'ID per un volume può essere `vol-1122AABB`. Quando utilizzi questo ID con l' EC2 API, devi cambiarlo in. `vol-1122aabb` In caso contrario, l' EC2 API potrebbe non funzionare come previsto.

> **Important**
>
> IDs per i volumi Storage Gateway e gli snapshot di Amazon EBS creati dai volumi gateway stanno passando a un formato più lungo. A partire da dicembre, tutti i nuovi volumi e istanze verranno creati con una stringa di 17 caratteri. A partire da aprile 2016, potrai utilizzarli più a lungo in IDs modo da poter testare i tuoi sistemi con il nuovo formato. Per ulteriori informazioni, consulta Longer EC2 e EBS Resource IDs.
>
> Ad esempio, un ARN volume con gli ID volume in formato più lungo sarà come la seguente: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
>
> Un ID snapshot con formato ID più lungo sarà come il seguente: `snap-78e226633445566ee`.
>
> Per ulteriori informazioni, vedere Annuncio: Heads-up — Longer Storage Gateway volume and snapshot IDs in arrivo nel 2016.

Etichettatura delle risorse di Storage Gateway

In Storage Gateway, puoi usare i tag per gestire le risorse. I tag consentono di aggiungere metadati alle risorse e di classificarle per renderle più facili da gestire. Ogni tag è composto da una coppia chiave-valore definita dall'utente. È possibile aggiungere i tag a gateway, volumi e nastri virtuali. Puoi cercare e filtrare queste risorse in base ai tag aggiunti.

Ad esempio, puoi usare i tag per identificare le risorse Storage Gateway utilizzate da ogni reparto dell'organizzazione. Puoi contrassegnare con i tag i gateway e i volumi utilizzati dal reparto contabile: (`key=department` e `value=accounting`). Puoi quindi filtrare con questo tag per identificare tutti i gateway e i volumi utilizzati dal reparto contabile e usare le informazioni per determinare i costi. Per ulteriori informazioni, consulta Utilizzo dei tag di allocazione dei costi e Utilizzo dell'editor di tag.

Se archivi un nastro virtuale contrassegnato da tag, il nastro mantiene i propri tag nell'archivio. Analogamente, se recuperi un nastro dall'archivio su un altro gateway, i tag sono gestiti nel nuovo gateway.

Per File Gateway, puoi utilizzare i tag per controllare l'accesso alle risorse. Per informazioni su come eseguire questa attività, consultare Utilizzo dei tag per controllare l'accesso al gateway e alle risorse.

I tag non hanno alcun significato semantico ma vengono interpretati rigorosamente come stringhe di caratteri.

Le seguenti restrizioni si applicano ai tag:

- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Il numero massimo di tag per ogni risorsa è 50.
- Le chiavi dei tag non possono iniziare con `aws:`. Questo prefisso è riservato per l'uso di AWS .
- I caratteri validi per la proprietà di chiave sono lettere e numeri UTF-8, spazi e i caratteri speciali + - = . _ : / e @.

Lavorare con i tag

È possibile lavorare con i tag utilizzando la console Storage Gateway, l'API di Storage Gateway o l'interfaccia a riga di comando (CLI) Storage Gateway. Le procedure seguenti illustrano come aggiungere, modificare ed eliminare un tag dalla console.

Per aggiungere un tag

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione, scegliere la risorsa a cui vuoi applicare un tag.

   Ad esempio, per applicare tag a un gateway, scegliere Gateways (Gateway), quindi scegliere il gateway che si desidera contrassegnare con dei tag dall'elenco di gateway.
3. Scegliere Tags (Tag), quindi Add tag (Aggiungi tag).
4. Nella finestra di dialogo Add/edit tags (Aggiungi/Modifica tag), selezionare Add New Volume (Aggiungi nuovo volume).
5. Digita una chiave per Key (Chiave) e un valore per Value (Valore). Ad esempio, è possibile digitare **`Department`** per la chiave e **`Accounting`** per il valore.

> **Note**
>
> È possibile lasciare la casella Value (Valore) vuota.

6. Per aggiungere altri tag, scegliere Create Tag (Crea tag). È possibile aggiungere più tag a una risorsa.
7. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

Per modificare un tag

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegliere la risorsa con il tag da modificare.
3. Scegliere Tags (Tag) per aprire la finestra di dialogo Add/edit tags (Aggiungi/modifica tag).
4. Scegli l'icona a forma di matita accanto al tag che desideri modificare, quindi modifica il tag.
5. Al termine della modifica dei tag, scegliere Save (Salva).

Come Per eliminare un tag

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegliere la risorsa con il tag da eliminare.
3. Scegliere Tags (Tag), quindi scegliere Add/edit tags (Aggiungi/modifica tag) per aprire la finestra di dialogo Add/edit tags (Aggiungi/modifica tag).
4. Scegliere l'icona X accanto al tag che si desidera eliminare, poi scegliere Save (Salva).

Utilizzo di componenti open source per Gateway di archiviazione AWS

Questa sezione descrive gli strumenti e le licenze di terze parti da cui dipendiamo per fornire Gateway di archiviazione AWS funzionalità.

Argomenti

- Componenti open source per Storage Gateway
- Componenti open source per Amazon S3 File Gateway

Componenti open source per Storage Gateway

Vengono utilizzati diversi strumenti e licenze di terze parti per fornire funzionalità per Volume Gateway, Tape Gateway e Amazon S3 File Gateway.

Utilizza i seguenti link per scaricare il codice sorgente di alcuni componenti software open source inclusi nel software: Gateway di archiviazione AWS

- Per i dispositivi Storage Gateway distribuiti su VMware ESXi: sources.tar
- Per i dispositivi Storage Gateway distribuiti su Microsoft Hyper-V: sources_hyperv.tar
- Per le appliance Storage Gateway distribuite su una macchina virtuale (KVM) basata su kernel Linux: sources_KVM.tar

Questo prodotto include software sviluppato dal progetto OpenSSL per l'utilizzo nel kit di strumenti OpenSSL (http://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consulta Licenze di terze parti.

Componenti open source per Amazon S3 File Gateway

Per fornire la funzionalità di Amazon S3 File Gateway (S3 File Gateway) vengono utilizzati diversi strumenti e licenze di terze parti.

Utilizza i seguenti link per scaricare il codice sorgente di alcuni componenti software open source inclusi nel software S3 File Gateway:

- Per Amazon S3 File Gateway: 3-open-source.tgz sgw-file-s

Questo prodotto include software sviluppato dal progetto OpenSSL per l'utilizzo nel kit di strumenti OpenSSL (http://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consulta Licenze di terze parti.

Quote per le condivisioni di file

La tabella seguente elenca le quote per le condivisioni dei file.

Description	Limite
Il numero massimo di condivisioni di file per il gateway **Note** Ogni condivisione di file può connettersi solo a un bucket S3, ma più condivisioni di file possono connettersi allo stesso bucket. Se connetti più di una condivisione di file allo stesso bucket, devi configurare ogni condivisione di file in modo che utilizzi un nome di prefisso univoco e non sovrapposto per evitare conflitti. read/write Il numero di condivisioni di file gestite da un gateway può influire sulle prestazioni del gateway. Per ulteriori informazioni, consulta Guida alle prestazioni per gateway con più condivisioni di file.	50
Il numero massimo di file per i quali un gateway può memorizzare simultaneamente i metadati nella cache **Note** Poiché S3 File Gateway è supportato da Amazon S3, non esiste una dimensione massima delle cartelle o un limite al numero di file che è possibile archiviare o a cui è possibile accedere tramite un gateway. Ogni gateway ha un limite configurabile che determina il numero di file per	Capacità del gateway: Piccolo: 5 milioni di file Medio: 10 milioni di file Grande: 20 milioni di file

Description	Limite
i quali può memorizzare simultane amente i metadati nella cache. È possibile utilizzare l'azione UpdateGat ewayInformationAPI per GatewayCa pacityimpostare su `SmallMedium`, o. `Large` Questa impostazione influisce sulle prestazioni del gateway e sui consigli hardware. Per ulteriori informazioni, vedere Guida alle prestazioni per gateway con più condivisioni di file.	
La dimensione massima di un singolo file **Note** Se provi a scrivere file più grandi del limite di dimensione, pezzo per pezzo, verranno caricati solo i primi 5 TiB. Se si tenta di scrivere contempor aneamente i file più grandi del limite di dimensione, sui client Windows non viene creato alcun file e sui client Linux viene creato un file di dimensione zero.	5 TiB

Description	Limite
Lunghezza massima del percorso **Note** I client non sono autorizzati a creare un percorso che superi questa lunghezza; farlo genera un errore. Questo limite si applica a entrambi i protocolli supportati da File Gateway, NFS e SMB. La lunghezza del percorso in byte viene calcolata in base ai valori dei bit dei caratteri nella codifica UTF-8.	1024 byte
Lunghezza massima del nome del file **Note** File Gateway non supporta nomi di file che superano questa lunghezza. La lunghezza del nome di file in byte viene calcolata in base ai valori dei bit dei caratteri nella codifica UTF-8.	255 byte

Dimensioni disco locale consigliate per il gateway

La tabella seguente contiene le dimensioni consigliate per lo storage su disco locale per il gateway distribuito.

Tipo di gateway	Cache (minimo)	Cache (massimo)
Gateway di file S3	150 GiB	64 TiB

> **Note**
>
> È possibile configurare una o più unità locali per la cache fino alla capacità massima. Quando si aggiunge la cache a un gateway esistente, è importante creare nuovi dischi nell'host (hypervisor o istanza Amazon EC2). Non modificare le dimensioni dei dischi esistenti se i dischi sono stati precedentemente allocati come cache.

Utilizzo delle classi di archiviazione

Amazon S3 File Gateway supporta le classi di storage Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 One Zone-Infrequent Access, Amazon S3 Intelligent-Tiering e Amazon Glacier. Per ulteriori informazioni sulle classi di storage, consulta le classi di storage Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

> **Note**
>
> S3 File Gateway attualmente non supporta la classe di storage Amazon S3 Glacier Instant Retrieval.

Argomenti

- Utilizzo di classi di storage con un File Gateway
- Utilizzo della classe di archiviazione GLACIER con File Gateway

Utilizzo di classi di storage con un File Gateway

Quando si crea o si aggiorna una condivisione di file, è possibile selezionare una classe di archiviazione per gli oggetti. Puoi scegliere la classe di storage Amazon S3 Standard o una qualsiasi delle classi di storage S3 Standard-IA, S3 One Zone-IA o S3 Intelligent-Tiering. Gli oggetti archiviati in una qualsiasi di queste classi di storage possono essere trasferiti a GLACIER utilizzando una politica del ciclo di vita.

Classe di storage Amazon S3	Considerazioni
Standard	Selezionare Standard per archiviare i file ad accesso frequente in modo ridondante in più

Classe di storage Amazon S3	Considerazioni
	zone di disponibilità geograficamente distinte. Questa è la classe di storage predefinita. Per ulteriori dettagli, consulta i prezzi di Amazon S3.

Classe di storage Amazon S3	Considerazioni
S3 Intelligent-Tiering	Scegli Intelligent-Tiering per ottimizzare i costi di storage spostando automaticamente i dati nel livello di accesso allo storage più convenien te. Gli oggetti di dimensioni inferiori a 128 KB non sono idonei per il tiering automatico nella classe di storage Intelligent-Tiering. Questi oggetti vengono addebitati in base alle tariffe del livello di accesso frequente e non sono soggetti alla tariffa di monitoraggio addebitata per gli oggetti suddivisi su più livelli. S3 Intelligent-Tiering ora supporta un livello Archive Access e un livello Deep Archive Access. S3 Intelligent-Tiering sposta automatic amente gli oggetti a cui non si accede da 90 giorni al livello Archive Access e, dopo 180 giorni senza accesso, al livello Deep Archive Access. Ogni volta che un oggetto in uno dei livelli di accesso all'archivio viene ripristinato, l'oggetto passa al livello Frequent Access entro poche ore ed è pronto per essere recuperat o. Ciò crea errori di timeout per gli utenti o le applicazioni che cercano di accedere ai file tramite una condivisione di file se l'oggetto esiste solo in uno dei due livelli di archiviazione. Non utilizzate i livelli di archiviazione con S3 Intelligent-Tiering se le applicazioni accedono ai file tramite le condivisioni di file offerte dal File Gateway. Quando le operazioni sui file che aggiornan o i metadati (come proprietario, timestamp, autorizzazioni e ACLs) vengono eseguite su

Classe di storage Amazon S3	Considerazioni
	file gestiti da File Gateway, l'oggetto esistente viene eliminato e viene creata una nuova versione dell'oggetto in questa classe di storage Amazon S3. Verifica l'impatto delle operazioni sui file sulla creazione di oggetti prima di utilizzare questa classe di storage in produzione. Per ulteriori dettagli, consulta i prezzi di Amazon S3.

Classe di storage Amazon S3	Considerazioni
S3 Standard-IA	Selezionare Standard-IA per archiviare i dati degli oggetti ad accesso poco frequente in modo ridondante in più zone di disponibilità geograficamente distinte. Gli oggetti archiviati nella classe di storage Standard-IA possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione, la richiesta, il recupero o la transizione di oggetti tra classi di storage entro 30 giorni. È prevista una durata minima di archiviazione di 30 giorni. Gli oggetti eliminati prima di 30 giorni sono soggetti a un addebito proporzionale pari al costo di archiviazione per i giorni rimanenti. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Per gli oggetti di dimensioni inferiori a 128 KB viene addebitato il costo di 128 KB e vengono applicate le tariffe per l'eliminazione anticipata. Quando le operazioni sui file che aggiornan o i metadati (come proprietario, timestamp, autorizzazioni e ACLs) vengono eseguite su file gestiti da File Gateway, l'oggetto esistente viene eliminato e viene creata una nuova versione dell'oggetto in questa classe di storage Amazon S3. È necessario verificare l'impatto delle operazioni sui file sulla creazione di oggetti prima di utilizzare questa classe di storage in produzione, poiché si applicano le tariffe di eliminazione anticipata. Per ulteriori dettagli, consulta i prezzi di Amazon S3.

Classe di storage Amazon S3	Considerazioni
S3 One Zone-IA	Scegli One Zone-IA per archiviare i file a cui accedi meno frequentemente in un'unica zona di disponibilità. Gli oggetti archiviati nella classe di archiviazione One Zone-IA possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione, la richiesta, il recupero o la transizione di oggetti tra classi di archiviazione entro 30 giorni. È prevista una durata minima di archiviazione di 30 giorni e agli oggetti eliminati prima di 30 giorni viene applicato un addebito proporzionale pari al costo di archiviazione per i giorni rimanenti. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Per gli oggetti di dimensioni inferiori a 128 KB vengono addebitati i costi di 128 KB e vengono applicate le tariffe per l'eliminazione anticipata. Quando le operazioni sui file che aggiornano i metadati (come proprietario, timestamp, autorizzazioni e ACLs) vengono eseguite su file gestiti da File Gateway, l'oggetto esistente viene eliminato e viene creata una nuova versione dell'oggetto in questa classe di storage Amazon S3. È necessario verificare l'impatto delle operazioni sui file sulla creazione di oggetti prima di utilizzare questa classe di storage in produzione, poiché si applicano le tariffe di eliminazione anticipata. Per ulteriori dettagli, consulta i prezzi di Amazon S3.

Sebbene sia possibile scrivere oggetti direttamente da una condivisione di file nella classe di storage S3-Standard-IA, S3-One Zone-IA o S3 Intelligent-Tiering, ti consigliamo di utilizzare una politica del ciclo di vita per la transizione degli oggetti anziché scrivere direttamente dalla condivisione di file, soprattutto se prevedi di aggiornare o eliminare l'oggetto entro 30 giorni dall'archiviazione. Per informazioni sulla politica del ciclo di vita, consulta Gestione del ciclo di vita degli oggetti.

Utilizzo della classe di archiviazione GLACIER con File Gateway

Se esegui la transizione di un file ad Amazon Glacier tramite le politiche del ciclo di vita di Amazon S3 e il file è visibile ai client di condivisione file tramite la cache, si verificheranno I/O degli errori durante l'aggiornamento del file. Ti consigliamo di configurare CloudWatch Events per ricevere notifiche quando si verificano questi I/O errori e di utilizzare la notifica per agire. Ad esempio, puoi intervenire per ripristinare l'oggetto archiviato su Amazon S3. Dopo che gli oggetti sono ripristinati su S3, i client della condivisione file possono accedervi e aggiornarli tramite la condivisione file.

Per informazioni su come ripristinare oggetti archiviati, consulta Restoring archived objects nella Amazon Simple Storage Service User Guide.

> **Important**
>
> S3 File Gateway non supporta ufficialmente la classe di storage S3 Glacier Instant Retrieval. Sebbene sia possibile designare oggetti in un bucket di condivisione di file per S3 Glacier Instant Retrieval utilizzando policy relative al ciclo di vita o PUT richieste dirette, S3 File Gateway non è in grado di riconoscere quali file si trovano in quella classe di storage ed eseguirà operazioni sui file su di essi come qualsiasi altro oggetto. Poiché S3 Glacier Instant Retrieval ha costi di accesso più elevati rispetto ad altre classi di storage Amazon S3, le operazioni di massa sui file, come scansioni antivirus e ridenominazioni`rsync`, possono comportare costi elevati per Amazon S3 se non vengono gestite con attenzione. Per questo motivo, non consigliamo di utilizzare S3 Glacier Instant Retrieval con S3 File Gateway.

Utilizzo dei driver Kubernetes Container Storage Interface

Kubernetes è un sistema open source per automatizzare l'implementazione, la scalabilità e la gestione delle applicazioni containerizzate. In un ambiente Kubernetes, un contenitore è simile a una macchina virtuale, ma ha proprietà di isolamento rilassate per condividere il sistema operativo (OS) tra le sue applicazioni. Pertanto, i contenitori sono considerati più leggeri di. VMs Analogamente a una macchina virtuale, un contenitore ha il proprio filesystem, una quota di CPU allocata, memoria,

spazio di processo e altro ancora. Poiché sono disaccoppiati dall'infrastruttura sottostante, sono portatili tra cloud e distribuzioni di sistemi operativi. Se disponi di un cluster Kubernetes, puoi installare e configurare i driver Kubernetes Container Storage Interface (CSI) tra le istanze del cluster per consentire loro di utilizzare un Amazon S3 File Gateway esistente per lo storage.

Dopo aver installato i driver CSI per il tipo di condivisione di file che desideri utilizzare, devi creare uno o più oggetti di storage. A seconda del tipo di provisioning che desideri che Kubernetes utilizzi quando i tuoi pod richiedono l'archiviazione, devi creare un singolo oggetto Kubernetes o sia un oggetto che un *`StorageClass`* *`PersistentVolume`* oggetto per connettere i pod di calcolo Kubernetes alla tua *`PersistentVolumeClaim`* condivisione di file. Per https://kubernetes.io/docs/concepts/storage/ ulteriori informazioni, consulta la documentazione online di Kubernetes all'indirizzo.

Argomenti

- Lavorare con i driver CSI SMB
- Utilizzo dei driver NFS CSI

Lavorare con i driver CSI SMB

Segui le procedure in questa sezione per installare, configurare o eliminare i driver CSI necessari per utilizzare una condivisione di file SMB su un Amazon S3 File Gateway per lo storage nel tuo cluster Kubernetes. Per ulteriori informazioni, consulta la documentazione del driver SMB CSI open source all'indirizzo. GitHub https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md

> **Note**
>
> Quando si crea un `PersistentVolume` oggetto o un `StorageClass` oggetto, è possibile specificare un `ReclaimPolicy` parametro per determinare cosa succede allo storage esterno quando gli oggetti vengono eliminati. Il driver CSI SMB supporta le `Recycle` opzioni `Retain` and, ma attualmente non supporta alcuna opzione. `Delete`

Installa i driver

Per installare i driver CSI di Kubernetes SMB:

1. Da un terminale a riga di comando con accesso al tuo cluster Kubernetes, `kubectl` esegui il seguente comando:

curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. Attendi il completamento del comando precedente, quindi usa i seguenti comandi per assicurarti che i driver pod CSI siano in esecuzione:

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   L'output visualizzato dovrebbe essere simile al seguente:

```
NAME                                 READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-smb-controller-56bfddd689-dh5tk  4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4  4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                   3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                   3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Crea un oggetto SMB StorageClass

Per creare un nuovo StorageClass oggetto SMB per il tuo cluster Kubernetes:

1. Crea un file di configurazione denominato `storageclass.yaml` con contenuti simili all'esempio seguente. Sostituisci le tue informazioni specifiche sulla distribuzione con quelle mostrate. *`ExampleValues`*

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
```

```
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub
 directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. Da un terminale a riga di comando con accesso e, esegui il seguente comando: `kubectl storageclass.yaml`

   kubectl apply -f storageclass.yaml

   > **Note**
   >
   > Puoi anche crearlo StorageClass fornendo il testo di `.yaml` configurazione del passaggio precedente alla maggior parte delle piattaforme di gestione e containerizzazione Kubernetes di terze parti.

3. Configura i pod nel tuo cluster Kubernetes per utilizzare quelli nuovi che hai creato. StorageClass Per ulteriori informazioni, consulta la documentazione online di Kubernetes all'indirizzo. https://kubernetes.io/docs/concepts/storage/

Crea SMB e oggetti PersistentVolume PersistentVolumeClaim

Per creare nuovi SMB PersistentVolume e PersistentVolumeClaim oggetti:

1. Crea due file di configurazione. Uno con nome `persistentvolume.yaml` e uno con nome`persistentvolumeclaim.yaml`.
2. Per`persistentvolume.yaml`, aggiungi contenuti simili all'esempio seguente. Sostituisci le tue informazioni specifiche sulla distribuzione con quelle mostrate. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
        driver: smb.csi.k8s.io
        readOnly: false
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. Per`persistentvolumeclaim.yaml`, aggiungete contenuti simili all'esempio seguente. Sostituisci le tue informazioni specifiche sulla distribuzione con quelle mostrate. *ExampleValues*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
```

```
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
name of the PersistentVolume you created
        storageClassName: ""
```

4. Da un terminale a riga di comando con accesso a entrambi `kubectl` i `.yaml` file creati, esegui i seguenti comandi:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > Puoi anche creare PersistentVolumeClaim gli oggetti PersistentVolume and fornendo il testo di `.yaml` configurazione del passaggio precedente alla maggior parte delle piattaforme di gestione e containerizzazione Kubernetes di terze parti.

5. Configura i pod nel tuo cluster Kubernetes per utilizzare quelli nuovi che hai creato. PersistentVolumeClaim Per ulteriori informazioni, consulta la documentazione online di Kubernetes all'indirizzo. https://kubernetes.io/docs/concepts/storage/

Disinstalla i driver

Per disinstallare i driver CSI di Kubernetes SMB:

- Da un terminale a riga di comando con accesso al tuo cluster Kubernetes, `kubectl` esegui il seguente comando:

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

Utilizzo dei driver NFS CSI

Segui le procedure in questa sezione per installare, configurare o eliminare i driver CSI necessari per utilizzare una condivisione di file NFS su un Amazon S3 File Gateway per lo storage nel tuo cluster Kubernetes. Per ulteriori informazioni, consulta la documentazione del driver NFS CSI open source

su at. GitHub https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md

Installa i driver

Per installare i driver Kubernetes NFS CSI:

1. Da un terminale a riga di comando con accesso al tuo cluster Kubernetes, `kubectl` esegui il seguente comando:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --

2. Attendi il completamento del comando precedente, quindi usa i seguenti comandi per assicurarti che i driver pod CSI siano in esecuzione:

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   L'output visualizzato dovrebbe essere simile al seguente:

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-nfs-controller-56bfddd689-dh5tk       4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4       4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                        3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-dr4s4                        3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Create un oggetto NFS StorageClass

Per creare un StorageClass oggetto NFS per il tuo cluster Kubernetes:

1. Crea un file di configurazione denominato `storageclass.yaml` con contenuti simili all'esempio seguente. Sostituisci le tue informazioni specifiche sulla distribuzione con quelle mostrate. *`ExampleValues`*

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: example-nfs-classname
    namespace: example-namespace
provisioner: nfs.csi.k8s.io
parameters:
    server: gateway-dns-name-or-ip-address
    share: /example-share-name
reclaimPolicy: Retain
volumeBindingMode: Immediate
mountOptions:
    - hard
    - nfsvers=4.1
```

2. Da un terminale a riga di comando con accesso e, esegui il seguente comando: `kubectl storageclass.yaml`

   kubectl apply -f storageclass.yaml

   > **Note**
   >
   > Puoi anche crearlo StorageClass fornendo il testo di `.yaml` configurazione del passaggio precedente alla maggior parte delle piattaforme di gestione e containerizzazione Kubernetes di terze parti.

3. Configura i pod nel tuo cluster Kubernetes per utilizzare il nuovo oggetto che hai creato. StorageClass Per ulteriori informazioni, consulta la documentazione online di Kubernetes all'indirizzo. https://kubernetes.io/docs/concepts/storage/

Crea NFS e oggetti PersistentVolume PersistentVolumeClaim

Per creare nuovi NFS PersistentVolume e PersistentVolumeClaim oggetti:

1. Crea due file di configurazione denominati `persistentvolume.yaml` `epersistentvolumeclaim.yaml`.

2. Per `persistentvolume.yaml`, aggiungete contenuti simili all'esempio seguente. Sostituisci le tue informazioni specifiche sulla distribuzione con quelle mostrate. *ExampleValues*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
            share: /example-share-name
```

3. Per `persistentvolumeclaim.yaml`, aggiungete contenuti simili all'esempio seguente. Sostituisci le tue informazioni specifiche sulla distribuzione con quelle mostrate. *ExampleValues*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
```

```
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name
of the PersistentVolume you created
    storageClassName: ""
```

4. Da un terminale a riga di comando con accesso a entrambi `.yaml` i file, esegui `kubectl` i seguenti comandi:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > Puoi anche creare PersistentVolumeClaim gli oggetti PersistentVolume and fornendo il testo di `.yaml` configurazione del passaggio precedente alla maggior parte delle piattaforme di gestione e containerizzazione Kubernetes di terze parti.

5. Configura i pod nel tuo cluster Kubernetes per utilizzare il nuovo oggetto che hai creato. PersistentVolumeClaim Per ulteriori informazioni, consulta la documentazione online di Kubernetes all'indirizzo. https://kubernetes.io/docs/concepts/storage/

Disinstalla i driver

Per disinstallare i driver Kubernetes NFS CSI:

- Da un terminale a riga di comando con accesso al tuo cluster Kubernetes, `kubectl` esegui il seguente comando:

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/uninstall-driver.sh | bash -s master --

Gateway di archiviazione AWS Modulo Terraform

HashiCorpTerraform è un motore Infrastructure as Code (IaC) open source sviluppato utilizzando il HashiCorp Configuration Language (HCL). Terraform fornisce un flusso di lavoro coerente con interfaccia a riga di comando (CLI) che, insieme ad Amazon S3 File Gateway per l'infrastruttura di back-end, può gestire centinaia di servizi cloud e codificare il cloud in file di configurazione dichiarativi. APIs

Puoi usare Terraform per distribuire in sicurezza un Amazon S3 File Gateway come macchina virtuale (VM) nella tua infrastruttura virtuale locale. Terraform fornisce l'automazione per l'infrastruttura virtuale locale. Consulta Automatizza le implementazioni di Amazon S3 File Gateway con Terraform HashiCorp by per informazioni sulla distribuzione rapida di un Amazon S3 File Gateway utilizzando Terraform all' VMware interno di un ambiente virtuale locale. VMware

> **Note**
>
> Potrebbe essere necessario configurare Terraform per ottenere l'ultima versione dell'immagine della macchina per la tua piattaforma hypervisor preferita. Gateway di archiviazione AWS Le immagini delle macchine Storage Gateway utilizzano la seguente convenzione di denominazione. Il numero di versione aggiunto al nome dell'immagine cambia con ogni versione rilasciata.
>
> `aws-storage-gateway-FILE_S3-1.25.0`

Questa automazione ti fornisce un modulo Terraform personalizzabile che puoi utilizzare per fornire un Amazon S3 File Gateway con tutte le risorse e le dipendenze necessarie per implementare completamente il gateway e le condivisioni di file nel tuo ambiente VM. Il modulo Terraform fornisce la VM del gateway, attiva il gateway, configura il disco della cache, unisce il gateway a un dominio, crea i bucket Amazon S3, crea le condivisioni di file e le mappa su bucket. Per un esempio completo di repository che contiene codice Terraform per creare le risorse necessarie per eseguire Amazon S3 File Gateway in locale, consulta il codice sorgente del modulo Terraform Storage Gateway su. GitHub

> **Note**
>
> Il modulo Amazon S3 File Gateway per Terraform è un'iniziativa supportata dalla comunità. Non fa parte di un AWS servizio. Il miglior supporto è fornito dalla community di AWS Storage.

Riferimento API per Storage Gateway

Oltre a utilizzare la console, puoi utilizzare l' Gateway di archiviazione AWS API per configurare e gestire i gateway in modo programmatico. Questa sezione descrive Gateway di archiviazione AWS le operazioni, la richiesta di firma per l'autenticazione e la gestione degli errori. Per ulteriori informazioni sulle regioni e sugli endpoint disponibili per Storage Gateway, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.

> **Note**
>
> È inoltre possibile utilizzare il AWS SDKs per sviluppare applicazioni con Storage Gateway. AWS SDKs Per Java, .NET e PHP racchiudono l'API Storage Gateway sottostante, semplificando le attività di programmazione. Per ulteriori informazioni sul download delle librerie SDK, consulta Librerie e codice di esempio.

Argomenti

- Gateway di archiviazione AWS Intestazioni di richiesta obbligatorie
- Firmare le richieste
- Risposte agli errori
- Azioni API Storage Gateway

Gateway di archiviazione AWS Intestazioni di richiesta obbligatorie

Questa sezione descrive le intestazioni richieste a cui è necessario inviare con ogni richiesta POST. Gateway di archiviazione AWS Devi includere intestazioni HTTP per identificare le informazioni principali sulla richiesta, tra cui l'operazione che vuoi richiamare, la data della richiesta e le informazioni che indicano la tua autorizzazione come mittente della richiesta. Le intestazioni fanno distinzione tra maiuscole e minuscole, ma l'ordine delle intestazioni non è importante.

L'esempio seguente mostra le intestazioni utilizzate nell'ActivateGatewayoperazione.

```
POST / HTTP/1.1
```

```
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

Di seguito sono riportate le intestazioni da includere nelle richieste POST a. Gateway di archiviazione AWS Le intestazioni mostrate di seguito che iniziano con «x-amz» sono intestazioni specifiche. AWS Tutte le altre intestazioni elencate sono intestazioni comuni usate in transazioni HTTP.

Header	Descrizione
`Authorization`	L'intestazione di autorizzazione contiene diverse informazioni sulla richiesta che consentono di determinare se la richiesta è un'azione valida Gateway di archiviazione AWS per il richiedente. Il formato di questa intestazione è il seguente (con l'aggiunta di interruzioni di riga ai fini della leggibilità): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` Nella sintassi precedente, si specificano l'anno YourAccessKey, il mese e il giorno (aaaammgg), la regione e il. CalculatedSignature Il formato dell'intestazione di autorizzazione è dettato dai requisiti del processo di firma V4. AWS I dettagli sulla firma vengono approfonditi nell'argomento Firmare le richieste.
`Content-Type`	Utilizza `application/x-amz-json-1.1` come tipo di contenuto per tutte le richieste di. Gateway di archiviazione AWS `Content-Type: application/x-amz-json-1.1`

Header	Descrizione
`Host`	Utilizza l'intestazione host per specificare l' Gateway di archiviazione AWS endpoint a cui inviare la richiesta. Ad esempio, `storagegateway.us-east-2.amazonaws.com` è l'endpoint per la regione Stati Uniti orientali (Ohio). Per ulteriori informazioni sugli endpoint disponibili per Gateway di archiviazione AWS, consulta Gateway di archiviazione AWS Endpoints and Quotas in. Riferimenti generali di AWS `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	È necessario fornire il timestamp nell'intestazione HTTP `Date` o nell'intestazione AWS `x-amz-date` . (Alcune librerie client HTTP non consentono di impostare l'intestazione `Date`) Quando è presente un'`x-amz-date` intestazione, Gateway di archiviazione AWS ignora qualsiasi `Date` intestazione durante l'autenticazione della richiesta. Il `x-amz-date` formato deve essere ISO86 01 Basic nel formato YYYYMMDD' T'HHMMSS'Z'. Se vengono utilizzati sia l'intestazione che, il `Date` formato dell'`x-amz-date` intestazione Date non deve essere 01. ISO86 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	Questa intestazione specifica la versione dell'API e l'operazione richiesta . I valori dell'intestazione target sono formati concatenando la versione API con il nome API e usano il formato seguente. `x-amz-target: StorageGateway_ APIversion .operationName` Il valore OperationName (ad esempio ActivateGateway "«) può essere trovato dall'elenco delle API,. Riferimento API per Storage Gateway

Firmare le richieste

Storage Gateway richiede l'autenticazione con firma di ogni richiesta inviata. Per firmare una richiesta, è necessario calcolare una firma digitale utilizzando una funzione hash crittografica. Una funzione hash crittografica è una funzione che restituisce un valore hash univoco basato sull'input. L'input alla funzione hash include il testo della richiesta e la tua chiave di accesso segreta. La funzione hash restituisce un valore hash che includi nella richiesta come firma. La firma è parte dell'intestazione `Authorization` della richiesta.

Dopo aver ricevuto la richiesta, Storage Gateway ricalcola la firma utilizzando la stessa funzione hash e lo stesso input utilizzati per firmare la richiesta. Se la firma risultante corrisponde alla firma nella richiesta, Storage Gateway elabora la richiesta. In caso contrario, la richiesta viene respinta.

Storage Gateway supporta l'autenticazione con AWS Signature Version 4. La procedura per il calcolo di una firma può essere suddivisa in tre fasi:

- Fase 1. Creazione di una richiesta canonica

  Riorganizza la richiesta HTTP in un formato canonico. L'utilizzo di un formato canonico è necessario in quanto Storage Gateway utilizza quel formato quando ricalcola una firma da confrontare con quella che hai inviato.

- Fase 2: creazione di una stringa di firma

  Crea una stringa che utilizzerai come uno dei valori di input per la funzione hash crittografica. La stringa, denominata stringa di firma, è una concatenazione del nome dell'algoritmo hash, della data della richiesta, di una stringa di ambito credenziali e della richiesta in formato canonico creata nella fase precedente. La stringa di ambito credenziali è anch'essa una concatenazione di data, regione e informazioni sul servizio.

- Fase 3. Creazione di una firma

  Crea una firma per la tua richiesta utilizzando una funzione hash crittografica che accetta due stringhe di input: la tua stringa di firma e una chiave derivata. La chiave derivata viene calcolata partendo dalla chiave di accesso segreta e utilizzando la stringa di ambito delle credenziali per creare una serie di codici di autenticazione dei messaggi basati su Hash ()HMACs.

Esempio di calcolo di firma

L'esempio in questa sezione mostra come creare una firma per ListGateways. L'esempio può essere utilizzato come riferimento per verificare il metodo di calcolo della firma.

L'esempio presuppone quanto segue:

- Il timestamp della richiesta è "Mon, 10 Sep 2012 00:00:00" GMT.
- L'endpoint è la regione Stati Uniti orientali (Ohio).

La sintassi generale della richiesta (incluso il corpo JSON) è:

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

Il formato canonico della richiesta calcolata per Fase 1. Creazione di una richiesta canonica è:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

L'ultima riga della richiesta canonica è l'hash del corpo della richiesta. Nota inoltre la terza riga vuota nella richiesta canonica. Questo perché non esistono parametri di query per questa API (o per alcun Storage Gateway APIs).

La stringa di firma per Fase 2: creazione di una stringa di firma è:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

La prima riga della stringa di firma è l'algoritmo, la seconda è il timestamp, la terza è l'ambito credenziali e l'ultima è un hash del formato della richiesta canonica in Fase 1.

Per Fase 3. Creazione di una firma, la chiave derivata può essere rappresentata come segue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Se viene utilizzata la chiave di accesso segreta wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, la firma calcolata è:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

La fase finale consiste nel creare l'intestazione `Authorization`. Per la chiave di accesso AKIAIOSFODNN7EXAMPLE, l'intestazione (con interruzioni di riga aggiunte per facilitare la lettura) è:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Risposte agli errori

Argomenti

- Eccezioni
- Codici di errore delle operazioni
- Risposte agli errori

Questa sezione fornisce informazioni di riferimento sugli Gateway di archiviazione AWS errori. Questi errori sono rappresentati da un'eccezione di errore e da un codice di errore dell'operazione.

L'eccezione di errore `InvalidSignatureException`, ad esempio, viene restituita da qualsiasi risposta API in caso di problema con la firma della richiesta. Tuttavia, il codice di errore dell'operazione `ActivationKeyInvalid` viene restituito solo per l'ActivateGatewayAPI.

A seconda del tipo di errore, Storage Gateway può restituire solo un'eccezione oppure sia un'eccezione che un codice di errore dell'operazione. In Risposte agli errori vengono forniti esempi di risposte di errore.

Eccezioni

La tabella seguente elenca le eccezioni Gateway di archiviazione AWS API. Quando un' Gateway di archiviazione AWS operazione restituisce una risposta di errore, il corpo della risposta contiene una di queste eccezioni. `InternalServerError` e `InvalidGatewayRequestException` restituiscono uno dei messaggi Codici di errore delle operazioni dei codici di errore delle operazioni che forniscono il codice di errore dell'operazione specifico.

Eccezione	Messaggio	Codice di stato HTTP
`IncompleteSignatureException`	La firma specificata non è completa.	400 Richiesta non valida
`InternalFailure`	L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto sconosciuto.	500 - Errore interno del server
`InternalServerError`	Uno dei messaggi dei codici di errore delle operazioni in Codici di errore delle operazioni.	500 - Errore interno del server
`InvalidAction`	L'azione o operazione richiesta non è valida.	400 Richiesta non valida
`InvalidClientTokenId`	Il certificato X.509 o AWS l'ID della chiave di accesso fornito non esiste nei nostri archivi.	403 Non consentito

Eccezione	Messaggio	Codice di stato HTTP
`InvalidGatewayRequestException`	Uno dei messaggi dei codici di errore delle operazioni in Codici di errore delle operazioni.	400 Richiesta non valida
`InvalidSignatureException`	La firma di richiesta che abbiamo calcolato non corrisponde alla firma che hai fornito. Controlla la tua chiave di AWS accesso e il metodo di firma.	400 Richiesta non valida
`MissingAction`	Nella richiesta manca un parametro di un'azione o un'operazione.	400 Richiesta non valida
`MissingAuthenticationToken`	La richiesta deve contenere un ID chiave di AWS accesso valido (registrato) o un certificato X.509.	403 Non consentito
`RequestExpired`	La richiesta ha superato la data di scadenza o la data della richiesta (con margine di 15 minuti) oppure la data della richiesta è oltre 15 minuti nel futuro.	400 Richiesta non valida
`SerializationException`	Si è verificato un errore durante la serializzazione. Controllare che il formato del payload JSON sia corretto.	400 Richiesta non valida
`ServiceUnavailable`	La richiesta non è riuscita a causa di un errore temporaneo del server.	503 Service Unavailable (503 Servizio non disponibile)
`SubscriptionRequiredException`	L' AWS Access Key Id richiede un abbonamento per il servizio.	400 Richiesta non valida

Eccezione	Messaggio	Codice di stato HTTP
`ThrottlingException`	Velocità superata.	400 Richiesta non valida
`TooManyRequests`	Troppe richieste.	429 Troppe richieste
`UnknownOperationException`	È stata specificata un'operazione sconosciuta. Le operazioni valide sono elencate in Azioni API Storage Gateway.	400 Richiesta non valida
`UnrecognizedClientException`	Il token di sicurezza incluso nella richiesta non è valido.	400 Richiesta non valida
`ValidationException`	Il valore di un parametro di input è errato o non compreso nell'intervallo.	400 Richiesta non valida

Codici di errore delle operazioni

La tabella seguente mostra la mappatura tra i codici di errore Gateway di archiviazione AWS operativi e APIs che può restituire i codici. Tutti i codici di errore delle operazioni vengono restituiti con una delle due eccezioni generali `InternalServerError` e `InvalidGatewayRequestException` descritte in Eccezioni.

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`ActivationKeyExpired`	La chiave di attivazione specificata è scaduta.	ActivateGateway
`ActivationKeyInvalid`	La chiave di attivazione specificata non è valida.	ActivateGateway

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`ActivationKeyNotFound`	La chiave di attivazione specificata non è stata trovata.	ActivateGateway
`BandwidthThrottleScheduleNotFound`	La limitazione di larghezza di banda specificata non è stata trovata.	DeleteBandwidthRateLimit
`CannotExportSnapshot`	Lo snapshot specificato non può essere esportato.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	L'iniziatore specificato non è stato trovato.	DeleteChapCredentials
`DiskAlreadyAllocated`	Il disco specificato è già allocato.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	Il disco specificato non esiste.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskSizeNotGigAligned`	Il disco specificato non è allineato ai gigabyte.	CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`DiskSizeGreaterThanVolumeMaxSize`	La dimensione del disco specificata è superiore alla dimensione massima del volume.	CreateStorediSCSIVolume
`DiskSizeLessThanVolumeSize`	La dimensione del disco specificata è inferiore alla dimensione del volume.	CreateStorediSCSIVolume
`DuplicateCertificateInfo`	Le informazioni sul certificato specificate sono duplicate.	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	La configurazione dell'endpoint dell'associazione di file system esistente è in conflitto con la configurazione specificata.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	L'indirizzo IP dell'endpoint specificato è già in uso.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	Manca l'indirizzo IP dell'endpoint di File System Association.	AssociateFileSystem
FileSystemAssociationNotFound	L'associazione di file system specificata non è stata trovata.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
FileSystemNotFound	Il file system specificato non è stato trovato.	AssociateFileSystem

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayInternalError`	Si è verificato un errore interno del gateway.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayNotConnected`	Il gateway specificato non è connesso.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayNotFound`	Il gateway specificato non è stato trovato.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayProxyNetworkConnectionBusy`	La connessione di rete proxy gateway specificata è occupata.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`InternalError`	Si è verificato un errore interno.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`InvalidParameters`	La richiesta specificata contiene parametri non validi.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`LocalStorageLimitExceeded`	Il limite di storage locale è stato superato.	AddCache AddUploadBuffer AddWorkingStorage
`LunInvalid`	Il LUN specificato non è valido.	CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`MaximumVolumeCountExceeded`	Il numero massimo di volumi è stato superato.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	La configurazione di rete del gateway è stata modificata.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`NotSupported`	L'operazione specifica ta non è supportata.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	Il gateway specificato non è aggiornato.	ActivateGateway
`SnapshotInProgressException`	Lo snapshot specificato è in corso.	DeleteVolume
`SnapshotIdInvalid`	Lo snapshot specificato non è valido.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`StagingAreaFull`	L'area di gestione temporanea è piena.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`TargetAlreadyExists`	La destinazione specificata esiste già.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	La destinazione specificata non è valida.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	La destinazione specificata non è stata trovata.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`UnsupportedOperationForGatewayType`	L'operazione specificata non è valida per il tipo di gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Il volume specificato esiste già.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	Il volume specificato non è valido.	DeleteVolume
`VolumeInUse`	Il volume specificato è già in uso.	DeleteVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`VolumeNotFound`	Il volume specificato non è stato trovato.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	Il volume specificato non è pronto.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Risposte agli errori

Quando si verifica un errore, le informazioni dell'intestazione della risposta contengono:

- Tipo di contenuto: application/ -1.1 x-amz-json
- Un codice di stato HTTP `4xx` o `5xx` appropriato

Il corpo di una risposta di errore contiene informazioni relative all'errore. La risposta di errore di esempio seguente mostra la sintassi di output degli elementi della risposta comuni a tutte le risposte di errore.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

La tabella seguente illustra i campi della risposta di errore JSON mostrata nella sintassi precedente.

__type

Una delle eccezioni elencate in Eccezioni.

Tipo: stringa

error

Contiene dettagli dell'errore specifici dell'API. Negli errori generali, ovvero non specifici di un'API, queste informazioni sull'errore non vengono visualizzate.

Tipo: raccolta

errorCode

Uno dei codici di errore delle operazioni .

Tipo: stringa

errorDetails

Questo campo non viene usato nella versione corrente dell'API.

Tipo: stringa

message

Uno dei messaggi dei codici di errore delle operazioni.

Tipo: stringa

Esempi di risposta di errore

Il seguente corpo JSON viene restituito se si utilizza l' DescribeStorediSCSIVolumesAPI e si specifica un input di richiesta ARN del gateway che non esiste.

```
{
  "__type": "InvalidGatewayRequestException",
```

```
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
}
```

Il corpo JSON seguente viene restituito se Storage Gateway calcola una firma che non corrisponde alla firma inviata con una richiesta.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Azioni API Storage Gateway

Per un elenco delle operazioni di Storage Gateway , consulta Operazioni nel Riferimento API Gateway di archiviazione AWS .

Cronologia dei documenti per la Guida per l'utente di Amazon S3 File Gateway

La tabella seguente descrive le modifiche importanti apportate in ogni versione di questa guida per l'utente dopo aprile 2018. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile iscriversi a un feed RSS.

Modifica	Descrizione	Data
IPv6 supporto	IPv6il supporto è disponibile per le versioni 2.x o successive delle appliance gateway.	10 settembre 2025
Sono state aggiunte linee guida per la produttività e l'ottimizzazione	Il capitolo sulle prestazioni e l'ottimizzazione include ora consigli e best practice per massimizzare il throughput di S3 File Gateway e ottimizzare la distribuzione per i casi d'uso di backup del database SQL Server. Per ulteriori informazioni, consulta Massimizzazione della velocità effettiva di S3 File Gateway e Ottimizzazione di S3 File Gateway per i backup dei database SQL Server.	13 giugno 2025
È stata aggiunta la funzionalità di report sulla cache	S3 File Gateway può ora generare un report dei metadati per i file attualmente presenti nella cache di caricamento locale per una condivisione di file specifica. Per ulteriori informazioni, consulta Creare un rapporto	31 marzo 2025

	sulla cache per S3 File Gateway, Visualizzare e gestire i report sulla cache per S3 File Gateway e Comprensione delle informazioni fornite nei report sulla cache di S3 File Gateway.	
È stato aggiunto il supporto per la crittografia lato server a doppio livello con AWS KMS chiavi (DSSE-KMS)	Ora puoi utilizzare la crittografia lato server a doppio livello con AWS KMS chiavi per crittografare i file che S3 File Gateway carica su Amazon S3. Per ulteriori informazioni su DSSE-KMS, consulta Crittografare gli oggetti archiviati da File Gateway in Amazon S3.	13 settembre 2024
È stata aggiunta l'opzione per attivare o disattivare gli aggiornamenti di manutenzione	Storage Gateway riceve aggiornamenti di manutenzione regolari che possono includere aggiornamenti del sistema operativo e del software, correzioni per la stabilità, le prestazioni e la sicurezza e l'accesso a nuove funzionalità. È ora possibile configurare un'impostazione per attivare o disattivare questi aggiornamenti per ogni singolo gateway della distribuzione. Per ulteriori informazioni, vedere Gestione degli aggiornamenti del gateway tramite la Gateway di archiviazione AWS console .	6 giugno 2024

È stato aggiunto un nuovo livello di sicurezza SMB	S3 File Gateway ora supporta un livello di sicurezza aggiuntivo che puoi utilizzare per applicare la crittografia AES a 256 bit per le connessioni client SMB. Per ulteriori informazioni, consulta Impostare un livello di sicurezza per il gateway.	23 maggio 2024
Rapporti sulla versione del software dell'appliance Gateway e note di rilascio per S3 File Gateway	Sono state aggiunte note di rilascio per descrivere le funzionalità, i miglioramenti e le correzioni nuovi e aggiornati inclusi in ogni versione dell'appliance Amazon S3 File Gateway. È possibile determinare il numero di versione del software di un gateway dalla console di Storage Gateway o utilizzando il AWS CLI. Per ulteriori informazioni, vedere Release Notes — Gateway Appliance Software.	5 ottobre 2023

Allarmi consigliati CloudWatch aggiornati	L' CloudWatch `HealthNotifications` allarme ora si applica ed è consigliato per tutti i tipi di gateway e piattaforme host. Le impostazioni di configurazione consigliate sono state aggiornate anche per `HealthNotifications` e `AvailabilityNotifications`. Per ulteriori informazioni, vedere Comprensione degli CloudWatch allarmi Comprendere .	2 ottobre 2023
Aumento del numero massimo di condivisioni di file per gateway	S3 File Gateway ora supporta fino a 50 condivisioni di file per gateway, un aumento rispetto al precedente limite di 10. Ciò consente di creare più condivisioni di file su un singolo gateway, riducendo il numero di gateway da gestire. Per ulteriori informazioni, consulta Quote per le condivisioni di file.	18 gennaio 2023

È stato aggiunto il supporto per gli attributi DOS	S3 File Gateway ora supporta gli attributi DOS per i file archiviati in Amazon S3. Ciò consente di preservare gli attributi dei file di Windows come sola lettura, nascosto, sistema e archivio quando i file vengono caricati su Amazon S3. Per ulteriori informazioni, consulta Support per gli attributi dei file in Amazon S3 File Gateway.	18 gennaio 2023
Suggerimenti per la risoluzione dei problemi GatewayClockOutOfSync aggiunti	La sezione Risoluzione dei problemi relativi al File Gateway include ora linee guida per la risoluzione dei problemi che possono verificarsi se l'orologio del sistema gateway non è sincronizzato con l'ora del server AWS Storage Gateway. Per ulteriori informazioni, vedere Errore:. GatewayClockOutOfSync	19 ottobre 2022

È stata aggiunta la limitazione della larghezza di banda di rete basata sulla pianificazione	S3 File Gateway ora supporta la limitazione della larghezza di banda di rete basata sulla pianificazione per il caricamento dei dati su Amazon S3. Questa funzionalità consente di limitare la quantità di larghezza di banda di rete utilizzata dal gateway in periodi di tempo specifici, aiutandoti a gestire l'utilizzo della rete durante le ore lavorative di punta. Per ulteriori informazioni, consulta Gestione della larghezza di banda per S3 File Gateway.	18 gennaio 2022
Procedure di creazione del gateway aggiornate	La procedura per la creazione di un nuovo gateway è stata aggiornata per riflettere le modifiche nella console Storage Gateway. Per ulteriori informazioni, consulta Creare e attivare un Amazon S3 File Gateway.	12 ottobre 2021

Support per la chiusura forzata dei file nelle condivisioni di file SMB	È ora possibile utilizzare le impostazioni del gruppo locale per assegnare le autorizzazioni di amministratore del gateway. Gli amministratori del gateway possono utilizzare lo snap-in Cartelle condivise di Microsoft Management Console per forzare la chiusura dei file aperti e bloccati nelle condivisioni di file SMB. Per ulteriori informazioni, consulta Configurare i gruppi locali per il gateway.	12 ottobre 2021
Supporto dei log di controllo per le condivisioni di file NFS	È ora possibile configurare le condivisioni di file NFS per generare registri di controllo che forniscono dettagli sull'accesso degli utenti a file e cartelle all'interno di una condivisione di file. È possibile utilizzare questi registri per monitorare le attività degli utenti e intervenire se vengono identificati modelli di attività inappropriati. Per ulteriori informazioni, vedere Understanding File Gateway audit log.	12 ottobre 2021

Supporto per gli alias dei punti di accesso	Le condivisioni di file File Gateway possono ora connettersi allo storage Amazon S3 utilizzando alias di punti di accesso in stile bucket. Per ulteriori informazioni, consulta Creazione di una condivisione file.	12 ottobre 2021
Supporto per endpoint e punti di accesso VPC	Le condivisioni di file File Gateway possono ora connettersi ai bucket S3 tramite punti di accesso o endpoint di interfaccia nel tuo VPC basato su. AWS PrivateLink Per ulteriori informazioni, consulta Creazione di una condivisione file.	7 luglio 2021
Supporto per il blocco opportunistico	Le condivisioni di file File Gateway possono ora utilizzare il blocco opportunistico per ottimizzare la strategia di buffering dei file, il che migliora le prestazioni nella maggior parte dei casi, in particolare per quanto riguarda i menu contestuali di Windows. Per ulteriori informazioni, consulta Creare una condivisione di file SMB.	7 luglio 2021
Conformità agli standard FedRAMP	Storage Gateway è ora conforme a FedRAMP. Per ulteriori informazioni, vedere Convalida della conformità per Storage Gateway.	24 novembre 2020

Notifica di caricamento dei file per File Gateway	File Gateway ora fornisce una notifica di caricamento dei file, che avvisa quando un file è stato completam ente caricato su Amazon S3 da File Gateway. Per ulteriori informazioni, consulta Ricevere una notifica di caricamento di file.	9 novembre 2020
Enumerazione basata sull'accesso per File Gateway	File Gateway ora fornisce l'enumerazione basata sull'accesso, che filtra l'enumerazione di file e cartelle in una condivisione di file SMB in base a quella condivisa. ACLs Per ulteriori informazi oni, vedere Creazione di una condivisione di file SMB.	9 novembre 2020
Migrazione File Gateway	File Gateway ora fornisce un processo documenta to per la sostituzione di un File Gateway esistente con un nuovo File Gateway. Per ulteriori informazioni, vedere Sostituzione di un File Gateway con un nuovo File Gateway.	30 ottobre 2020
Le prestazioni di lettura della cache a freddo di File Gateway sono aumentate di 4 volte	Storage Gateway ha aumentato di 4 volte le prestazioni di lettura della cache fredda. Per ulteriori informazioni, vedere Guida alle prestazioni per File Gateways.	31 agosto 2020

Ordinare l'appliance hardware tramite la console	È ora possibile ordinare l'appliance hardware tramite la Gateway di archiviazione AWS console. Per ulteriori informazioni, vedere Utilizzo dell'appliance hardware AWS Storage Gateway.	12 agosto 2020
Supporto per gli endpoint Federal Information Processing Standard (FIPS) in nuove regioni AWS	È ora possibile attivare un gateway con endpoint FIPS nelle regioni Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon) e Canada (Centrale). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.	31 luglio 2020

Support per più condivisioni di file collegate a un singolo bucket Amazon S3	File Gateway ora supporta la creazione di più condivisioni di file per un singolo bucket S3 e la sincronizzazione della cache locale di File Gateway con un bucket basato sulla frequenza di accesso alla directory. Puoi limitare il numero di bucket necessari per gestire le condivisioni di file che crei sul tuo File Gateway. Puoi definire più prefissi S3 per un bucket S3 e mappare un singolo prefisso S3 a una singola condivisi one di file gateway. È inoltre possibile definire nomi di condivisione di file del gateway indipendenti dal nome del bucket, in modo da soddisfare la convenzione di denominaz ione delle condivisioni di file locali. Per ulteriori informazi oni, vedere Creazione di una condivisione di file NFS o Creazione di una condivisione di file SMB.	7 luglio 2020

Aumento del quadruplo dello storage nella cache locale di File Gateway	Storage Gateway ora supporta una cache locale fino a 64 TB per File Gateway, migliorando le prestazioni per le applicazioni locali fornendo un accesso a bassa latenza a set di dati di lavoro più grandi. Per ulteriori informazioni, vedere Dimensioni dei dischi locali consigliate per il gateway nella Guida per l'utente di Storage Gateway.	7 luglio 2020
Visualizza gli CloudWatch allarmi Amazon nella console Storage Gateway	È ora possibile visualizzare gli CloudWatch allarmi nella console Storage Gateway. Per ulteriori informazioni, vedere Comprendere gli CloudWatch allarmi.	29 maggio 2020
Supporto per gli endpoint Federal Information Processing Standard (FIPS)	Puoi ora attivare un gateway con endpoint FIPS nelle regioni AWS GovCloud (US) . Per scegliere un endpoint FIPS per un File Gateway, vedi Scelta di un endpoint di servizio.	22 maggio 2020
Nuove regioni AWS	Storage Gateway è ora disponibile nelle regioni Africa (Città del Capo) ed Europa (Milano). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.	07 maggio 2020

Supporto per classe di storage S3 Intelligent-Tiering	Storage Gateway ora supporta la classe di archiviazione S3 Intelligent-Tiering. La classe di storage S3 Intelligent-Tiering è progettata per ottimizzare i costi dello storage spostando automaticamente i dati sul livello di accesso di storage più conveniente, senza impatto sulle prestazioni o sovraccarico operativo. Per ulteriori informazioni, consulta Classe di archiviazione per l'ottimizzazione automatica degli oggetti a cui si accede frequentemente e raramente nella Guida per l'utente di Amazon Simple Storage Service.	30 aprile 2020
Nuova AWS regione	Storage Gateway è ora disponibile nella regione AWS GovCloud (Stati Uniti orientali). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS in Riferimenti generali di AWS.	12 marzo 2020

Supporto per hypervisor macchina virtuale basata su kernel (KVM) Linux	Storage Gateway offre ora la possibilità di distribuire un gateway on-premise nella piattaforma di virtualizzazione KVM. I gateway distribuiti in KVM hanno tutte le stesse funzionalità e caratteristiche dei gateway on-premise esistenti. Per ulteriori informazioni, consulta l'argomento relativo agli Hypervisor supportati e requisiti host nella Guida per l'utente di Storage Gateway.	4 febbraio 2020
Support per VMware vSphere High Availability	Storage Gateway ora fornisce supporto per l'alta disponibilità per aiutare VMware a proteggere i carichi di lavoro di storage da guasti hardware, hypervisor o di rete. Per ulteriori informazioni, vedere Using VMware vSphere High Availability with Storage Gateway nella Storage Gateway User Guide. Questa versione include inoltre i miglioramenti delle prestazioni. Per ulteriori informazioni, consulta Prestazioni nella Guida per l'utente di Storage Gateway.	20 novembre 2019

Support per Amazon CloudWatch Logs	Ora puoi configurare File Gateway con Amazon CloudWatch Log Groups per ricevere notifiche sugli errori e sullo stato del gateway e delle sue risorse. Per ulteriori informazioni, consulta Getting Notified About Gateway Health and Errors with Amazon CloudWatch Log Groups nella Storage Gateway User Guide.	4 settembre 2019
Novità Regione AWS	Storage Gateway è ora disponibile nella regione Asia Pacifico (Hong Kong). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS in Riferimenti generali di AWS.	14 agosto 2019
Novità Regione AWS	Storage Gateway è ora disponibile nella regione Medio Oriente (Bahrein). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS in Riferimenti generali di AWS.	29 luglio 2019

Supporto per attivare un gateway in un cloud privato virtuale (VPC, Virtual Private Cloud)	È ora possibile attivare un gateway in un cloud privato virtuale. È possibile creare una connessione privata tra l'applicazione software locale e l'infrastruttura di storage basato sul cloud. Per ulteriori informazioni, vedere Activating a Gateway in a Virtual Private Cloud.	20 giugno 2019
Supporto per la condivisione di file SMB per Microsoft Windows ACLs	Per i File Gateway, ora puoi utilizzare le liste di controllo degli accessi di Microsoft Windows (ACLs) per controllare l'accesso alle condivisioni di file Server Message Block (SMB). Per ulteriori informazioni, vedere Utilizzo di Microsoft Windows ACLs per controllare l'accesso a una condivisione di file SMB.	8 maggio 2019
Supporto File Gateway per l'autorizzazione basata su tag	File Gateway ora supporta l'autorizzazione basata su tag. È possibile controllare l'accesso alle risorse File Gateway in base ai tag presenti su tali risorse. È inoltre possibile controllare l'accesso in base ai tag che possono essere trasmessi in una condizione di richiesta IAM. Per ulteriori informazioni, consulta Controllo dell'accesso alle risorse del gateway di file.	4 marzo 2019

Disponibilità dell'appliance hardware AWS Storage Gateway in Europa	L'appliance hardware AWS Storage Gateway è ora disponibile in Europa. Per ulteriori informazioni, consulta Regioni hardware appliance Gateway di archiviazione AWS in Riferimenti generali di AWS. Inoltre, ora è possibile aumentare lo storage utilizzabile sullo Storage Gateway Hardware Appliance da 5 TB a 12 TB e sostituire la scheda di rete in rame installata con una scheda di rete in fibra ottica da 10 gigabit. AWS Per ulteriori informazioni, consulta Configurazione dell'appliance hardware.	25 febbraio 2019
Supporto per l'appliance hardware AWS Storage Gateway	L'appliance hardware AWS Storage Gateway include il software Storage Gateway preinstallato su un server di terze parti. È possibile gestire l'appliance dalla Console di gestione AWS. L'appliance può ospitare gateway di file, di nastri virtuali e di volumi. Per ulteriori informazioni, consulta Utilizzo dell'appliance hardware Storage Gateway.	18 settembre 2018

Supporto per il protocollo SMB (Server Message Block)	I gateway di file hanno aggiunto il supporto per il protocollo SMB (Service Message Block) alle condivisi oni file. Per ulteriori informazi oni, consulta Creazione di una condivisione file.	20 giugno 2018

Aggiornamenti precedenti

La tabella che segue descrive le modifiche importanti apportate a ogni versione della Gateway di archiviazione AWS Guida per l'utente prima di maggio 2018.

Modifica	Descrizione	Data della modifica
Support per la classe di storage S3 One Zone-IA	Per i File Gateway, ora puoi scegliere S3 One Zone-IA come classe di storage predefinita per le tue condivisioni di file. Usando questa classe di storage, puoi archiviare i dati degli oggetti in un'unica zona di disponibilità in Amazon S3. Per ulteriori informazioni, consulta Creazione di una condivisione file.	4 aprile 2018
Nuovo Regione AWS	Il gateway di nastri virtuali è ora disponibile nella regione Asia Pacifico (Singapore). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	3 Aprile 2018
Support per refresh cache notification, Requester Pays e bucket predefiniti per Amazon ACLs S3	Con i gateway di file puoi ora ricevere notifiche quando il gateway completa l'aggiornamento della cache per il bucket Amazon S3. Per ulteriori informazioni, vedere RefreshCache.html nello Storage Gateway API Reference. Per File Gateways, ora è possibile specificare che il richiedente o il lettore paghi i costi di accesso anziché il proprietario del bucket.	1 marzo 2018

Modifica	Descrizione	Data della modifica
	File Gateway ora può dare il pieno controllo dei file scritti al proprietario del bucket S3 mappato alla condivisione di file NFS. Per ulteriori informazioni, consulta Creazione di una condivisione file.	
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Europa (Parigi). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	18 dicembre 2017
Support per la notifica di caricamento dei file e l'individuazione del tipo MIME (Multipurpose Internet Mail Extension)	File Gateway ora può inviare notifiche quando tutti i file scritti nella condivisione di file NFS sono stati caricati su Amazon S3. Per ulteriori informazioni, vedere NotifyWhenUploadedlo Storage Gateway API Reference. File Gateway ora può indovinare il tipo MIME degli oggetti caricati in base alle estensioni dei file. Per ulteriori informazioni, consulta Creazione di una condivisione file.	21 Novembre 2017
Support per la versione VMware ESXi 6.5 di Hypervisor	Gateway di archiviazione AWS ora supporta la versione 6.5 di VMware ESXi Hypervisor. Questa si aggiunge alle versioni 4.1, 5.0, 5.1, 5.5 e 6.0. Per ulteriori informazioni, consulta Hypervisor supportati e requisiti di hosting.	13 settembre 2017
Supporto del gateway di file per l'hypervisor Microsoft Hyper-V	Puoi ora distribuire un gateway di file in un hypervisor Microsoft Hyper-V. Per informazioni, consulta Hypervisor supportati e requisiti di hosting.	22 giugno 2017

Modifica	Descrizione	Data della modifica
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Asia Pacifico (Mumbai). Per informazioni dettaglia te, consulta Regioni AWS che supportano Storage Gateway.	02 maggio 2017
Aggiornamenti alle impostazioni della condivisione file Supporto per l'aggiornamento della cache per le condivisioni file	I gateway di file aggiungono ora opzioni di montaggio alle impostazioni della condivisione file. Puoi ora impostare opzioni di squash e di sola lettura per la condivisione file. Per ulteriori informazioni, consulta Creazione di una condivisione file. I gateway di file possono ora individuare nel bucket Amazon S3 oggetti aggiunti o rimossi dall'ultima volta in cui il gateway ha elencato il contenuto del bucket e ha memorizzato nella cache i risultati. Per ulteriori informazioni, RefreshCacheconsulta l'API Reference.	28 marzo 2017
Support per File Gateway su Amazon EC2	Gateway di archiviazione AWS ora offre la possibili tà di implementare un File Gateway in Amazon EC2. Puoi avviare un File Gateway in Amazon EC2 utilizzan do lo Storage Gateway Amazon Machine Image (AMI) ora disponibile come AMI comunitaria. Per informazi oni su come creare un File Gateway e distribuirlo su un' EC2 istanza, consultaCrea e attiva un Amazon S3 File Gateway. Per informazioni su come avviare un'AMI File Gateway, vedereImplementa un EC2 host Amazon predefinito per S3 File Gateway. Inoltre, File Gateway ora supporta la configurazione del proxy HTTP. Per ulteriori informazioni, consulta Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP.	08 febbraio 2017

Modifica	Descrizione	Data della modifica
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Europa (Londra). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	13 dicembre 2016
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Canada (Centrale). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	08 dicembre 2016
Supporto per il gateway di file	Oltre ai gateway di volumi e ai gateway di nastri virtuali, Storage Gateway offre ora gateway di file. Un gateway di file combina un servizio e un'applia nce software virtuale, permettendoti di archiviare e recuperare oggetti in Amazon S3 tramite protocolli di file standard del settore, come NFS (Network File System). Il gateway permette l'accesso a oggetti in Amazon S3 come file in un punto di montaggio NFS.	29 Novembre 2016

Note di rilascio per il software dell'appliance gateway

Queste note di rilascio descrivono le funzionalità, i miglioramenti e le correzioni nuovi e aggiornati inclusi in ogni versione dell'appliance Amazon S3 File Gateway FSx Amazon Gateway. Ogni versione del software è identificata dalla data di rilascio e da un numero di versione univoco.

È possibile determinare il numero di versione del software di un gateway controllando la relativa pagina Dettagli nella console Storage Gateway o chiamando l'azione DescribeGatewayInformationAPI utilizzando un AWS CLI comando simile al seguente:

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

Il numero di versione viene restituito nel `SoftwareVersion` campo della risposta API.

> **Note**
>
> Un gateway non riporterà le informazioni sulla versione del software nelle seguenti circostanze:
>
> - Il gateway è offline.
> - Il gateway esegue un software precedente che non supporta la segnalazione delle versioni.
> - Il tipo di gateway non è S3 File Gateway.

Per ulteriori informazioni sugli aggiornamenti di S3 File Gateway FSx File Gateway, vedere Gestione degli aggiornamenti del gateway tramite la console Storage Gateway Managing Gateway Using the AWS Storage Gateway Console .

Gateway basati su Amazon Linux 2023 (AL2023)

La tabella seguente elenca le note di rilascio per i gateway basati su 023. AL2

> **Note**
>
> Le versioni 1.x.x del gateway non possono essere aggiornate alla 2.x.x.

Data di rilascio	Versione del software	Note di rilascio
2025-12-15	2.0.5	Aggiornamenti di manutenzione: • È stato risolto un problema relativo alla metrica della dimensione del disco principale. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-11-12	2.0.4	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-11-12	2.0.4	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-10-15	2.0.3	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2025-09-15	2.0.2	Aggiornamenti di manutenzione: • È stato risolto un problema che impediva la modifica della capacità del gateway. • È stato risolto un problema con l'`UpdateSMBLocalGroups` API. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-08-29	2.0.1	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni. • Versione iniziale per gateway locali.
21 agosto 2025	2.0.0	Funzionalità: • Versione iniziale del nuovo sistema operativo. • IPv6 Supporto aggiunto.

Gateway basati su Amazon Linux 2 (AL2)

La tabella seguente elenca le note di rilascio per i gateway basati su. AL2

Data di rilascio	Versione del software	Note di rilascio
2025-12-15	1,27,18	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-11-17	1,27,17	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-10-15	1,27,16	Aggiornamenti di manutenzione: • È stato risolto un problema nel registro Upload Rename Order. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-09-22	1,27,15	Aggiornamenti di manutenzione: • È stato risolto un problema nel registro Upload Rename Order.
15-09-2025	1,27,14	Aggiornamenti di manutenzione:

Data di rilascio	Versione del software	Note di rilascio
		• Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-08-21	1,27,13	Aggiornamenti di manutenzione: • Statistiche e metriche di sistema aggiunte per fornire informazioni più approfondite sulle prestazioni del gateway.
18/08/2025	1,27,12	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-08-11	1,27,11	Aggiornamenti di manutenzione: • È stato risolto un problema che S3 riguardava gli aggiornamenti dei metadati nell'ambito di operazioni sui file specifiche per alcuni gateway.

Data di rilascio	Versione del software	Note di rilascio
2025-07-15	1,27,10	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni. • Sono stati risolti i problemi relativi al registro Upload Rename Order per i gateway.
2025-06-23	1,227,9	Aggiornamenti di manutenzione: • Sono stati risolti i problemi relativi al registro Upload Rename Order per i gateway. • È abilitato il registro Upload Rename Order per i nuovi gateway. • È stato risolto il problema che impediva al gateway di gestire correttamente le operazioni di eliminazione dei file che non erano stati caricati correttamente.

Data di rilascio	Versione del software	Note di rilascio
2025-06-16	1,27,8	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-05-26	1,27,7	Aggiornamenti di manutenzione: • Problemi risolti per Rename Ordering. **Note** Questo problema riguarda solo alcuni gateway. Riceverai una notifica se il gateway deve essere aggiornato. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-05-15	1,227,6	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2025-04-28	1,227,5	Aggiornamenti di manutenzione: • Sono stati risolti i problemi relativi al registro degli ordini di caricamento e ridenominazione. • Sono stati aggiunti strumenti di debug per aiutare a determinare le cause dei problemi di caricamento. • Sono state aggiunte statistiche e metriche di sistema per una visione più approfondita delle prestazioni del gateway. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-04-14	1.27.4	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2025-04-01	1,27,3	Aggiornamenti di manutenzione: • Aggiornamento per la configurazione della registrazione del gateway. Non è richiesta alcuna azione da parte del cliente.

Data di rilascio	Versione del software	Note di rilascio
2025-03-17	1,27,2	Aggiornamenti di manutenzione: • È stata aggiunta un'azione API che rimuove i dati e i metadati di condivisione di file memorizzati nella cache per i file che non sono stati caricati dal gateway su Amazon S3. Account AWS Devi essere nella lista dei destinatari autorizzati per utilizzare questa funzione. Se il gateway ha problemi con il caricamento non riuscito dei file, Supporto AWS può sbloccare la funzione e fornire indicazioni sul suo utilizzo. • È stata aggiunta la funzionalità per i nuovi gateway di registrare l'ordine delle operazioni di ridenominazione degli oggetti e di caricamento. Questo aiuta a evitare che i file non vengano caricati su Amazon S3 dopo operazioni di ridenominazione ripetute o sovrapposte. • È stato risolto un problema relativo all'apertura involontaria delle porte da parte di SMB.

Data di rilascio	Versione del software	Note di rilascio
		• Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-02-17	1,27,1	Aggiornamenti di manutenzione: • Java 11 rimosso. • Aggiunta la funzione cache per Supporto l'uso. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2025-01-17	1.27.0	Funzionalità: • Cache Reports (disponibile a breve): software gateway aggiornato per supportare il lancio di una funzionalità imminente progettata per generare report sui metadati dei file attualmente memorizzati nella cache da un S3 File Gateway. Potrai utilizzare questi report per risolvere i problemi in caso di file che non vengono caricati dal gateway su Amazon S3. Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2025-01-09	1,269,9	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2024-12-18	1,26,8	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2024-11-18	1,26,7	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2024-10-17	1,226,6	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2024-09-30	1,26,5	Aggiornamenti di manutenzione: • È stato risolto un problema a causa del quale i gateway locali non consentivano i canali di supporto • Elementi del sistema operativo e del software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2024-09-16	1.26.3	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2024-08-21	1,26,1	Aggiornamenti di manutenzione: • È stato risolto un problema relativo alla registrazione.
19/08/2020	1,26,0	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2024-07-16	1.25.2	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2024-06-17	1.25.1	Aggiornamenti di manutenzione: • È stato risolto un problema con gli aggiornamenti quando si utilizza un proxy e il DNS è disabilitato. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2024-05-15	1,25,0	Funzionalità: • Aggiunta la possibilità di impostare la crittografia minima AES-128 o AES-256. Questa è solo una modifica al gateway e sarà disponibile nella console Storage Gateway in una prossima versione. • Maggiore rotazione dei log di sistema quando lo spazio su disco è insufficiente. In precedenza, la scrittura di log che riempiva il disco principale causava l'arresto del gateway. Ora, man mano che lo spazio diminuisce, il gateway libererà più spazio per i log più recenti eliminando i log più vecchi. • È stato aggiunto il percorso S3 nelle notifiche sanitarie per errori di caricamento dei file. In precedenza, le notifiche sanitarie mostravano solo il percorso del file sul gateway. Le notifiche ora mostrano il percorso per aiutare gli utenti a localizzare il file in S3.

Data di rilascio	Versione del software	Note di rilascio
		• Il servizio ora ignora i blocchi del backend durante le eliminazioni forzate della condivisione di file. In precedenza, le eliminazioni forzate si interrompevano senza alcuna spiegazione quando si verificavano dei blocchi. Le eliminazioni forzate ora continuano senza interruzioni in questi scenari. Aggiornamenti di manutenzione: • Aggiornato lo stack NFS. • Java 17 JRE aggiornato. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2024-04-15	1,24,5	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2024-04-01	1,24,4	Aggiornamenti di manutenzione: • Risolto il problema del componente Network Time Protocol (NTP) mancante.
2024-03-18	1,24,3	Aggiornamenti di manutenzione: • È stato risolto un problema relativo alle prestazioni di ricerca con distinzione tra maiuscole e minuscole. • È stato risolto un problema che causava l'arresto anomalo dei processi. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2024-01-12	1,24,2	Aggiornamenti di manutenzione: • Risolto il problema di registrazione SMB.
2023-12-27	1.24.1	Aggiornamenti di manutenzione: • Problema di stabilità SMB risolto.

Data di rilascio	Versione del software	Note di rilascio

2023-12-01	1,24,0	Funzionalità:
		• Stack SMB aggiornato.
		  • È stato aggiunto il supporto per la crittografia AES-256, oltre a varianti più sicure della crittogra fia e della firma AES-128 quando si utilizza un client SMB 3.1.1 che lo richiede.
		  • SMBv1 (LANMAN/C IFS) Le funzionalità di copia lato server e di espansione wildcard lato server sono state rimosse. SMBv2 (e non sono interessati SMBv3). Ciò può influire negativam ente sulle prestazioni di determinati SMBv1 carichi di lavoro. Se lo utilizzi SMBv1, ti consigliamo di migrare a o. SMBv2 SMBv3
		
		Aggiornamenti di manutenzi one:
		• Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2023-10-24	1.23.2	Aggiornamenti di manutenzione: • È stato risolto un problema relativo alla mancata connessione di Support Channel per determinati utenti.
2023-08-14	1,23,1	Aggiornamenti di manutenzione: • Server NTP aggiornato per utilizzare il server di sincronizzazione per nuovi gateway.

Data di rilascio	Versione del software	Note di rilascio
2023-06-12	1,23,0	Funzionalità: • Aumento dei thread di caricamento per alcuni account. AWS Aggiornamenti di manutenzione: • È stato risolto un problema di violazione dell'accesso su copie di grandi dimensioni. • È stato risolto un problema NFS. • Java 8 rimosso. • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.
2023-04-19	1,22,1	Aggiornamenti di manutenzione: • È stato risolto un problema relativo alla ridenominazione di cartelle e file.

Data di rilascio	Versione del software	Note di rilascio
2023-01-18	1,22,0	Funzionalità: • Aggiunto il supporto per gli attributi DOS. • È stato aumentato il numero di condivisioni di file supportate per gateway da 10 a 50. • È stato implementato un meccanismo di rilevamento dell'inclinazione dell'orologio per determinare quando un gateway e un servizio non sono sincronizzati. Aggiornamenti di manutenzione: • Stack SMB aggiornato.
2022-07-06	1,21,2	Aggiornamenti di manutenzione: • Sistema operativo ed elementi software aggiornati per migliorare la sicurezza e le prestazioni.

Data di rilascio	Versione del software	Note di rilascio
2022-02-16	1,21,1	Funzionalità: • Aggiunte nuove metriche per la ridenominazione e l'eliminazione nella cache. Aggiornamenti di manutenzione: • Risolti vari problemi.
18/01/2022	1,21,0	Funzionalità: • Aggiunte nuove metriche CloudWatch . • Aggiunta la limitazione della larghezza di banda per il caricamento dei dati.
12-12-12 2021	1,20,0	***URGENT UPDATE***: • Vulnerabilità Log4j risolta.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.